Borland® StarTeam® 2009

StarTeam Server-Hilfe

Borland®

Borland Software Corporation
8310 N Capital of Texas Hwy, Bldg 2, Ste 100
Austin, Texas 78731 USA
www.borland.com

Juni 2009
PDF

StarTeam-Server

StarTeam-Server

In diesem Abschnitt wird die Verwendung des StarTeam-Servers erläutert

In diesem Abschnitt

Erste Schritte
Dieser Abschnitt enthält grundlegende konzeptionelle Themen zum Software Change Management.

Konzepte
Dieser Abschnitt enthält alle konzeptionellen Themen.

Verfahren
Dieser Abschnitt beschreibt alle Aufgaben in Verbindung mit der Verwaltung und dem Einsatz von StarTeam.

Referenz
Dieser Abschnitt enthält alle Referenzthemen.

Erste Schritte

Vielen Dank, dass Sie sich für StarTeam entschieden haben!

Dieser Abschnitt enthält grundlegende konzeptionelle Themen zum Software Change Management.

In diesem Abschnitt

Einführung

In diesem Abschnitt erhalten Sie eine Einführung zu StarTeam.

In diesem Abschnitt

StarTeam installieren
Klicken Sie auf den Link zur PDF-Datei, in der die StarTeam-Installation beschrieben ist.

Lizenz - Übersicht
Dieses Thema beschreibt die Lizenzierungsoptionen für StarTeam.

Allgemeines zur Codeverwaltung
Dieses Thema behandelt die Codeverwaltung auf höherer Ebene.

StarTeam Produktübersicht
Dieses Thema beschreibt die Produkte, aus denen sich StarTeam zusammensetzt.

Übersicht über die Standard-StarTeam-Architektur
Dieses Thema bietet eine Übersicht über die Standard-StarTeam-Architektur.

StarTeamMPX-Komponenten
Dieses Thema beschreibt die Komponenten von StarTeamMPX.

StarTeam installieren

Die Installationsanweisungen für das Installieren von StarTeam-Produkten finden Sie unter *StarTeam installieren*. Um das Dokument anzuzeigen, wählen Sie **Start** ▸ **Programme** ▸ **Borland StarTeam** ▸ **StarTeam Cross-Platform Client 2009** ▸ **Dokumentation** ▸ **Installation** oder **Start** ▸ **Programme** ▸ **Borland StarTeam** ▸ **StarTeam Server 2009** ▸ **Dokumentation** ▸ **Installation**.

Lizenz - Übersicht

Dieses Thema erklärt die Lizenzierung für StarTeam, d. h., das Lizenzpaket, das Sie erwerben, und die unterschiedlichen Arten der verfügbaren Lizenzen, um zu ermitteln, wie viele Benutzer auf StarTeam zugreifen.

Lizenzpakete

StarTeam-Server kann als Enterprise- oder Enterprise Advantage-Server ausgeführt werden. Jede der genannten Versionen bietet dabei unterschiedliche Funktionen. Die Funktionen, auf die ein Client auf dem Server zugreifen kann, werden durch das von Ihnen erworbene Lizenzpaket festgelegt.

- Die Enterprise-Version bietet alle Funktionen der Standardversion sowie die Task-Komponente, mit der Eigenschaften aller Komponenten und von Web Client angepasst werden können.
- Die Enterprise Advantage-Version bietet alle Enterprise-Funktionen und zusätzlich die Anforderungskomponente, StarTeamMPX und die alternativen Eigenschaftseditoren, mit denen Sie benutzerdefinierte Formulare erstellen und mithilfe von Workflow-Regeln festlegen können, wie alle Elemente einer Komponente die verschiedenen Entwicklungsphasen durchlaufen.
- Evaluierungslizenzen werden bei der Installation des Servers automatisch installiert und aktiviert. Diese Lizenzen bieten die Funktionen, die auch verfügbar wären, wenn Sie eine Enterprise Advantage-Lizenz verwenden. Sie laufen jedoch nach einer bestimmten Anzahl Tagen ab.

Wenn Sie die registrierte Lizenz ändern, während ein Benutzer auf seiner Workstation ein StarTeam-Projekt geöffnet hat, wird die Änderung für diesen Benutzer wirksam, nachdem er das Projektfenster geschlossen und erneut geöffnet hat. Wenn Sie einen StarTeam-Server nach Verwendung einer Evaluierungslizenz für die Enterprise Advantage Version lizenzieren, ändert sich der Funktionsumfang. Wenn Sie beispielsweise in der Evaluierungsphase Anforderungen erstellt haben und den Server anschließend mit einer anderen als der Enterprise Advantage Version lizenzieren, wird das Register "Anforderungen" nicht mehr angezeigt.

Personengebundene Lizenzen, Lizenzen für gleichzeitige Benutzer und Borland-Lizenztypen

Anhand von Lizenzen wird festgelegt, wie viele Benutzer auf den StarTeam-Server zugreifen können. Benutzer verfügen entweder über *personengebundene Lizenzen* oder *Lizenzen für gleichzeitige Benutzer*.

Personengebundene Lizenzen können nur von den Benutzern verwendet werden, denen sie zugewiesen wurden. Wenn Sie beispielsweise über fünf personengebundene Benutzerlizenzen und 25 Lizenzen für gleichzeitige Benutzer verfügen, ist der Zugriff der fünf Benutzer mit personengebundenen Benutzerlizenzen auf den Server garantiert. Keine andere Person ist dazu berechtigt, ihre Lizenzen zu verwenden.

Eine Lizenz für gleichzeitige Benutzer kann von allen Benutzern verwendet werden, die nicht über eine personengebundene Lizenz verfügen. Benutzer beispielsweise, die über keine personengebundenen Lizenzen verfügen, erhalten Lizenzen für gleichzeitige Benutzer in der Reihenfolge ihrer Anmeldung. Nachdem alle Lizenzen für gleichzeitige Benutzer vergeben sind, erhalten Benutzer bei der Anmeldung die Meldung, dass gerade keine weiteren Lizenzen verfügbar sind. Sie können später einen erneuten Anmeldeversuch starten. Beachten Sie, dass der Cross-Platform-Client und der Web-Client Lizenzen separat verbrauchen.

Wenn Sie den Server zum ersten Mal registrieren, geben sie eine oder zwei Seriennummern ein: Eine für personengebundene Lizenzen und/oder eine für Lizenzen für gleichzeitige Benutzer. Wenn Sie mehrere Seriennummern verwenden, müssen sich alle auf dieselbe StarTeam-Edition beziehen, d. h. Enterprise oder Enterprise Advantage.

Sie können weitere personengebundene Lizenzen oder Lizenzen für gleichzeitige Benutzer hinzufügen. StarTeam-Server erkennt die Gesamtanzahl, indem es die von der jeweiligen Seriennummer oder der .slip-Datei bereitgestellten Lizenzen zusammenfasst. Man spricht in diesem Zusammenhang auch von Lizenzierung im Stack-Verfahren.

Sie können eine beliebige Anzahl von Benutzern hinzufügen oder importieren, der Zugriff auf den Server wird jedoch nur den Benutzern mit personengebundenen Lizenzen oder Benutzern gewährt, denen bei der Anmeldung Lizenzen für gleichzeitige Benutzer zugewiesen werden. Wenn Sie über personengebundene StarTeam-Lizenzen verfügen, müssen Sie diese im Dialogfeld **Benutzer-Manager** des Fensters "Serveradministration" bestimmten Benutzern zuweisen. Es wird davon ausgegangen, dass alle anderen Benutzer über StarTeam-Lizenzen für gleichzeitige Benutzer verfügen.

Wenn Sie über Borland-Lizenzen verfügen, müssen den Benutzern (egal ob sie personengebundene oder Lizenzen für gleichzeitige Benutzer besitzen) im Dialogfeld "Benutzer-Manager" die richtigen .slip-Dateien zugewiesen werden. Anstelle einer .slip-Datei kann einem Benutzer auch der Status *Nicht zugewiesen* zugewiesen werden.

Dem StarTeam-Serveradministrator wird automatisch eine personengebundene Lizenz zugewiesen, die nicht entfernt werden kann. Dabei handelt es sich um eine "kostenfreie" Lizenz, die nicht in der Anzahl der zur Verfügung stehenden personengebundenen Benutzerlizenzen enthalten ist.

StarTeam-Lizenzen verwenden

StarTeam-Server kann auf zwei Arten lizenziert werden:

- Mit internen StarTeam-Lizenzen, die auch als native Lizenzen bezeichnet werden
- Mit Borland-Lizenzen für Lizenzserver (BLS und FlexLM)

Wenn StarTeam-Benutzer auf eine Serverkonfiguration zuzugreifen versuchen, die von einer nicht registrierten StarTeam-Serverversion verwaltet wird, werden die oberen und unteren Teilfenster der StarTeam-Clients ohne Register angezeigt.

Folgende Lizenzen können für StarTeam-Server erworben werden: personengebundene Enterprise- bzw. Enterprise Advantage-Lizenzen oder Enterprise- bzw. Enterprise Advantage-Lizenzen für gleichzeitige Benutzer. Jeder Client kann auf jeden Server zugreifen, sofern der Benutzer auf dem Server registriert ist und über eine gültige Lizenz verfügt. Kunden wählen in der Regel nur eine Lizenzierungsmethode: die native StarTeam-Lizenzierung, die Lizenzierung über den Borland License Server oder die FlexLM-Lizenzierung. Eine Kombination der verschiedenen Methoden ist jedoch möglich. Die Lizenzierung wird nach der Produktinstallation ausgeführt. Sie können entweder einen Lizenzserver einrichten und die Lizenzdateien (.slip-Dateien) in den Ordner "\licences" (ein Unterordner des Installationsordners des StartTeam-Servers) kopieren oder mithilfe des StarTeam-Serveradministrationstool die nativen StarTeam-Lizenzen registrieren.

StarTeam-Server-Lizenzen können durch weitere Lizenzen ergänzt werden, solange die Lizenzschlüssel zur selben Edition gehören (Enterprise oder Enterprise Advantage). Bevor Sie die erste neue Lizenz eingeben, müssen Sie die Evaluierungslizenz löschen.

Wenn Sie den Server zum ersten Mal registrieren, geben sie eine oder zwei Seriennummern ein: Eine für personengebundene Lizenzen und/oder eine für Lizenzen für gleichzeitige Benutzer. Wenn Sie mehrere Seriennummern verwenden, müssen sich alle auf dieselbe StarTeam-Edition beziehen. Sie können weitere personengebundene Lizenzen oder Lizenzen für gleichzeitige Benutzer hinzufügen. StarTeam-Server erkennt die Gesamtanzahl, indem es die von der jeweiligen Seriennummer oder der .slip-Datei bereitgestellten Lizenzen zusammenfasst. Man spricht in diesem Zusammenhang auch von Lizenzierung im Stack-Verfahren.

Verwandte Konzepte

StarTeam Produktübersicht

Verwandte Verfahrensweisen

Server lizenzieren

Allgemeines zur Codeverwaltung

Dieses Thema beschreibt die Codeverwaltung auf höherer Ebene, einschließlich allgemeiner Informationen zur Codeverwaltung und zu Repositorys.

Grundlagen der Codeverwaltung

Jedes Codeverwaltungssystem besteht aus einem oder mehreren zentralisierten Repositorys und einer bestimmten Anzahl an Clients. Ein Repository ist eine Datenbank, die nicht nur die tatsächlichen Datendateien enthält, sondern auch die Struktur der von Ihnen definierten Projekte.

Die meisten Codeverwaltungssysteme folgen dem Konzept eines logischen Projekts, in dem Dateien in der Regel in einer oder mehreren Verzeichnisstrukturen gespeichert werden. Ein Codeverwaltungsprojekt kann zusätzlich zu anderen Dokumenten und Artefakten ein oder mehrere IDE-basierte Projekte enthalten. Das System erzwingt zudem seine eigene Benutzerauthentifizierung oder nutzt, sehr häufig, die Vorteile der vom zu Grunde liegenden Betriebssystem zur Verfügung gestellten Benutzerauthentifizierung. Dies ermöglicht es dem Codeverwaltungssystem, eine Audit-Protkollierung bzw. einen Snapshot der Aktualisierungen der einzelnen Dateien zu speichern. Indem nur die Unterschiede gespeichert werden, kann das Codeverwaltungssystem alle Änderungen mit minimalen Speicheranforderungen verfolgen. Wenn Sie eine vollständige Kopie Ihrer Datei anzeigen möchten, führt das System eine Zusammenführung der Unterschiede aus und zeigt diese Zusammenführung in einer Ansicht an. Auf der physischen Ebene werden diese Unterschiede in separaten Dateien gespeichert, bis Sie Ihre Aktualisierungen dauerhaft zusammenführen und sie festschreiben.

Dieser Ansatz ermöglicht es Ihnen und anderen Teammitgliedern, parallel und gleichzeitig in mehreren, gemeinsam genutzten Projekten zu arbeiten, ohne Gefahr zu laufen, dass die Code-Änderungen einzelner Teammitglieder durch die Änderungen anderer Mitglieder überschrieben werden. Codeverwaltungssysteme schützen in ihrer grundlegendsten Form vor Codekonflikten oder Verlust von frühen Quellen. Die meisten Codeverwaltungssysteme stellen Tools für die Verwaltung von Codedateien mit Ein- und Auscheckfunktionen, für die Konfliktbehebung und Berichtsfunktionen zur Verfügung. Die meisten Systeme enthalten weder eine Logik für die Konfliktbehebung noch Funktionen für die Build-Verwaltung.

In der Regel ermöglichen Codeverwaltungssysteme es Ihnen nur, Revisionen für textbasierte Dateien, z. B. Quellcodedateien, HTML- und XML-Dokumente, zu vergleichen und zusammenzuführen. StarTeam speichert Binärdateien, z. B. Bilder oder compilierten Code, in den Projekten, die Sie der Kontrolle unterstellen. Es ist jedoch nicht möglich, Revisionen von Binärdateien zu vergleichen oder zusammenzuführen. Wenn Sie über das Speichern und Abrufen bestimmter Revisionen dieser Dateitypen hinaus weitere Funktionen ausführen möchten, sollten Sie ein manuelles System erstellen, um die an diesen Dateien vorgenommenen Änderungen verfolgen zu können.

Grundlagen zum Repository

Codeverwaltungssysteme speichern Kopien von Quelltextdateien und Unterschieddateien in einer bestimmten Form von Datenbank-Repository. In einigen Systemen, z. B. CVS oder VSS, ist dieses Repository eine logische Struktur, die aus nur aus einer Tabelle bestehenden Datenbankdateien und Steuerdateien besteht. In anderen Systemen, z. B. StarTeam, sind die Repositorys Instanzen eines bestimmten Datenbankverwaltungssystems (DBMS), z. B. MS SQL Server oder Oracle.

Repositorys werden in der Regel auf einem Remote-Server gespeichert, mit dem mehrere Benutzer verbunden sein können, um gleichzeitig Dateien ein- und auszuchecken und andere Verwaltungsaufgaben durchzuführen.

Mit StarTeam erstellen Sie eine *Serverkonfiguration*, um ein Repository für StarTeam-Projekte festzulegen. Neu erstellte Projekte werden einer Serverkonfiguration zugewiesen. Der Server kann eine beliebige Anzahl von Serverkonfigurationen ausführen. Da jede Serverkonfiguration eine Datenbank verwenden muss, müssen Sie sicherstellen, dass Sie die Konnektivität nicht nur mit dem Server, sondern auch mit der Datenbankinstanz herstellen.

Verwandte Konzepte

StarTeam Produktübersicht
Übersicht über die Serverkonfiguration

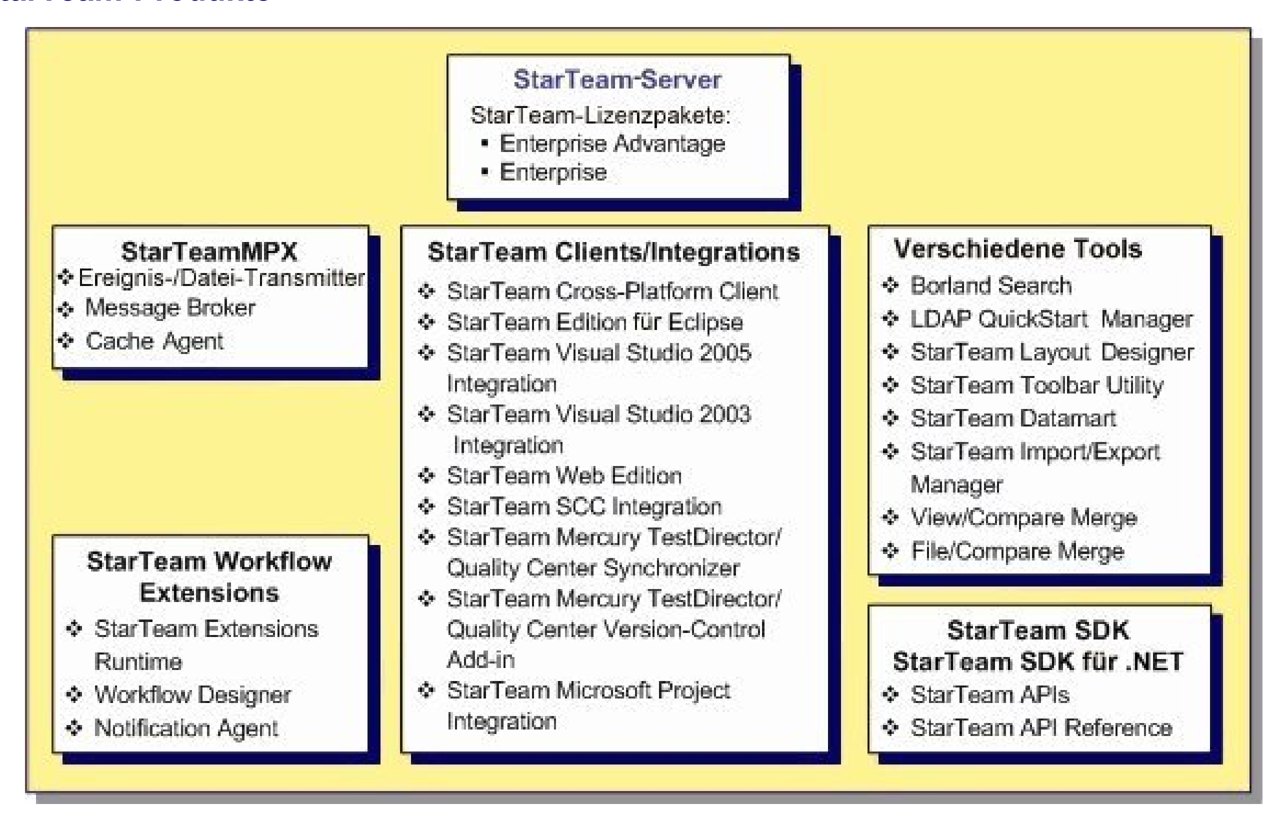
StarTeam Produktübersicht

Dieses Thema beschreibt die Produkte, aus denen sich StarTeam zusammensetzt. Die einzelnen Produkte sind in den folgenden Abschnitten beschrieben.

Die Produktbeschreibungen in den folgenden Abschnitten geben zudem an, ob das Produkt in einem bestimmten Lizenzpaket enthalten ist. StarTeam ist in zwei Lizenzpaketen verfügbar:

- **Enterprise:** StarTeam Enterprise bietet folgende grundlegende Funktionen: StarTeam-Server, StarTeamMPX (Ereignis-Transmitter und Message Broker), Cross-Platform-Client, Web-Client, LDAP Quick Start Manager und das SDK. Die Anforderungskomponente ist mit dieser Lizenz nicht verfügbar. Allerdings ermöglicht diese Lizenz den Zugriff auf benutzerdefinierte Felder.
- **Enterprise Advantage:** StarTeam Enterprise Advantage bietet alle StarTeam Enterprise-Funktionen und zusätzlich die Anforderungskomponente, StarTeamMPX (Cache-Agent und Datei-Transmitter) und StarTeam Workflow Extensions mit den alternativen Eigenschaftseditoren (APEs). Mit den APEs können Sie benutzerdefinierte Formulare erstellen und mithilfe von Workflow-Regeln festlegen, wie alle Elemente einer Komponente die verschiedenen Entwicklungsphasen durchlaufen.StarTeam Datamart kann separat erworben werden.

StarTeam-Produkte



Die StarTeam-Produktfamilie umfasst den StarTeam-Server, Cross-Platform Client, Web Client, StarTeamMPX, StarTeam Extensions, Tools und Dienstprogramme für die Verwendung mit den Clients und Servern, z. B. Borland Search, Borland LDAP QuickStart Manager, File Compare/Merge und StarTeam Datamart sowie eine Reihe von Integrationen mit Drittanbieterprodukten, einschließlich Integrationen mit Microsoft Visual Studio, Microsoft Project und der Microsoft SCC-Integration. Die einzelnen Produkte sind in den folgenden Abschnitten ausführlich beschrieben.

StarTeam-Server und Client-Workstations werden verbunden, um das Repository zu verwalten, an Dateien vorgenommene Änderungen zu speichern und Benutzern Zugriff auf Projektdaten zu gewähren.

StarTeam-Server

Verfügbar für Windows und Linux.

StarTeam-Server ist ein leistungsstarkes Tool zur Unterstützung verteilt arbeitender Entwicklungsteams und mobiler Teammitglieder. Er unterstützt Daten aller Sprachen, die in UTF-8 codiert werden können. Sie können auf die von StarTeam-Server verwalteten Daten mit einer Vielzahl von Clients zugreifen, z. B. dem Cross-Platform Client oder Web Client. Jeder Client muss über einen Benutzernamen und die benötigten Zugriffsrechte für die ausgewählte Serverkonfiguration (eine Instanz des StarTeam-Servers) verfügen.

StarTeam-Clients verwenden bekannte Anwendungen für den Zugriff auf den Server. Sie können beispielsweise mit Web Client über Internet Explorer auf den Server zugreifen. Wenn Sie eine StarTeam-IDE-Integration verwenden, können Sie aus IDE-Anwendungen, z. B. Microsoft Visual Studio und von Plattformen wie Eclipse heraus, auf den StarTeam-Server zugreifen.

Der Zugriff auf den StarTeam-Server kann lokal oder remote über das Internet, Intranet oder WAN erfolgen. Die integrierte Verschlüsselung gewährleistet ein sicheres Arbeiten über öffentliche Netze, z. B. das Internet. In der Regel wird der StarTeam-Server auf einem Computer installiert, auf den alle Mitglieder eines Teams Zugriff haben. Anschließend erfolgt die Einrichtung der StarTeam-Clients auf den Workstations der Teammitglieder.

StarTeamMPX

Verfügbar mit Enterprise-Lizenzen: Ereignis-Transmitter und Message Broker.

Verfügbar mit Enterprise Advantage-Lizenzen: Alle StarTeamMPX-Funktionen für Enterprise-Lizenzen und zusätzlich Datei-Transmitter und Cache Agent.

Dieses Produkt ist eine zusätzliche Option des StarTeam-Servers und muss separat installiert werden. Er verwendet das erweiterte Caching sowie die Publish/Subscribe-Kommunikationstechnologie, um die Leistung von StarTeam-Clients zu verbessern und die Skalierbarkeit von StarTeam-Server zu erweitern. Eine Linux-Version von StarTeamMPX ist ebenfalls verfügbar.

StarTeam Workflow Extensions

Verfügbar mit Enterprise Advantage-Lizenzen.

Mit StarTeam Workflow Extensions können Sie benutzerdefinierte Workflows für StarTeam-Komponenten, z. B. Änderungsanforderungen und Tasks, erstellen. Sie können den integrierten Workflow mithilfe von alternativen Eigenschaftseditoren (APEs), mit dem Workflow Designer und dem Notification Agent anpassen.

Alternative Eigenschaftseditoren (APEs)	APEs sind in Java geschriebene Formulare, die die standardmäßigen Eigenschaftdialogfelder ersetzen, die in den einzelnen Komponenten (Dateien, Änderungsanforderungen usw.) der Anwendung enthalten sind.
Workflow Designer	StarTeam enthält einen eigenen integrierten Workflow. Wenn Sie Ihren eigenen benutzerdefinierten Workflow verwenden möchten, können Sie diesen mit Workflow Designer entwickeln. Workflow Designer gibt Dateien des Typs *Elementtyp.Workflow.xml* aus, die die Schritte in einem Workflow formalisieren, und legt fest, wer in den einzelnen Schritten des Workflows beispielsweise zu Exceptions usw. benachrichtigt werden soll. Jede **.Workflow.xml*-Datei kann für ein gesamtes Projekt oder einzelne Ansichten in diesem Projekt

	verwendet werden. Die StarTeam Extensions-Workflow-Engine und der Notification Agent lesen die Informationen aus den von Workflow Designer generierten **.Workflow.xml*-Dateien.
Notification Agent	Notification Agent überwacht Serverkonfigurationen, um die Benutzer zu ermitteln, die über ausstehende Arbeiten und zu im Workflow-Prozess aufgetretenen Exceptions informiert werden müssen.

Cross-Platform-Client

Verfügbar mit beiden Lizenzen.

Der 2001 eingeführte Cross-Platform Client ist ein reiner Java-Client, der Unterstützung für Betriebssysteme zur Verfügung stellt, auf denen ein kompatibles JRE oder JDK verfügbar ist. In einem solchen Fall ist der Cross-Platform Client für die Windows-, Solaris- und Linux-Betriebssysteme verfügbar. In der StarTeam-Version wurde der Cross-Platform Client in vielen Bereichen qualitativ verbessert.

StarTeam Edition für Eclipse

Verfügbar mit beiden Lizenzen.

Mit StarTeam Edition für Eclipse können Sie Projekte auf dem StarTeam-Server und Projekte im Eclipse-Arbeitsbereich gemeinsam nutzen, es ist jedoch viel mehr als nur ein Plug-In für die Versionskontrolle. Diese Integration bietet Projektteams eine anpassbare Lösung mit Anforderungs-, Task- und Änderungsmanagement, Fehlerprotokollierung und Diskussionsverläufen, die nahtlos in die Eclipse-Plattform integriert sind.

StarTeam Visual Studio Integration

Das StarTeam Visual Studio Integration bietet die Funktionen der StarTeam-Software zur Konfigurationsverwaltung, die nahtlos in die Visual Studio-Entwicklungsumgebung integriert sind. Mit dieser Integration können Sie Anwendungen in der Visual Studio-Umgebung entwickeln und gleichzeitig die Versionskontroll-, Änderungsanforderungs, Thema-, Task und Anforderungskomponenten von StarTeam verwenden. Die Integration stellt die wichtigsten StarTeam-Menübefehle, Kontextmenübefehle und einen eingebetteten StarTeam-Client (der ein ähnliches Erscheinungsbild und viele Funktionen der vollständigen Cross-Platform Client-Installation enthält) in der Visual Studio-Entwicklungsumgebung zur Verfügung.

StarTeamWeb Client

Der neue StarTeam Web Client ist eine intuitive, webbasierte Schnittstelle, anhand der viele Benutzer gleichzeitig mit einem oder mehreren StarTeam-Servern eine Verbindung herstellen können, um auf Projekte zugreifen und Elemente verwalten zu können. Diese erste Web Client-Version enthält Kernfunktionen, die speziell auf Benutzer abgestimmt sind, die StarTeam-Änderungsanforderungen, -Anforderungen, -Tasks und -Themen anzeigen, erstellen und bearbeiten müssen. Das Durchsuchen von Dateien und eine begrenzte Anzahl an Dateioperationen stehen außerdem zur Verfügung.

Hinweis: Zum Einsatz des Web-Clients benötigen Sie eine StarTeam-Benutzerlizenz.

StarTeam SCC Integration

Verfügbar mit beiden Lizenzen.

Das StarTeam SCC Integration funktioniert mit jeder Anwendung, die die API (Application Programming Interface) der Microsoft-Quellcodeverwaltung (SCC) verwendet. Diese API, ursprünglich von Microsoft entwickelt, damit

Anwendungen mit Microsoft Visual SourceSafe arbeiten können, ermöglicht es Ihnen, Versionskontrolloperationen, z. B. das Ein- und Auschecken von Dateien, mit StarTeam als SCC-Provider auszuführen.

StarTeam Synchronizer für Mercury TestDirector für Quality Center

Dieses Produkt ist mit beiden Lizenzen verfügbar.

StarTeam Synchronizer für Mercury TestDirector für Quality Center stellt sicher, dass in Quality Center und einer von StarTeam-Server verwendeten Datenbank dieselben Daten verwendet werden. Das Ziel der Synchronisierung ist es, den Zugriff auf die aktuellsten Informationen zu Defekten zu ermöglichen, unabhängig davon, ob diese in Quality Center oder in StarTeam bearbeitet werden. Sie können Quality Center verwenden, um Defekte hinzuzufügen und Sie können mit StarTeam angeben, dass diese Defekte behoben wurden und umgekehrt. Für Teammitglieder ist es nicht wichtig zu wissen, wo der Defekt zuletzt bearbeitet wurde. Wenn die Synchronisierung der Datenbanken regelmäßig durchgeführt wird, sind immer die aktuellsten Daten verfügbar.

StarTeam-Versionskontroll-Add-In für Mercury TestDirector für Quality Center

Verfügbar mit beiden Lizenzen.

Das StarTeam Versionkontroll-Add-In für Mercury TestDirector für Quality Center ermöglicht Ihnen, aktuelle und vorherige Versionen von Quality Center-Testplänen unter Versionskontrolle im StarTeam-Repository abzulegen. Es unterstützt sowohl die Windows- als auch die Linux-Version des StarTeam-Servers.

StarTeam Microsoft Project Integration

Verfügbar mit beiden Lizenzen.

Die Interoperation zwischen StarTeam Microsoft Project Integration und Microsoft Project erleichtert die Arbeit der Projektplaner und Teammitglieder. Projektplaner verwenden Microsoft Project zur Erfassung der Vorgänge, die die Projektmitarbeiter erledigen müssen. Nach dem Exportieren der Vorgänge in StarTeam können sie mit StarTeam Informationen dazu sammeln, welche Arbeiten die einzelnen Teammitglieder in StarTeam durchgeführt haben. So müssen sie dies nicht einzeln mit den Teammitgliedern besprechen.

Borland Search

Verfügbar mit Enterprise Advantage-Lizenzen.

Mit Borland Search können Benutzer server- und projektübergreifende Ad-hoc-Abfragen ausführen. Die Abfrageergebnisse sind abhängig von den Zugriffsrechten des bei Borland Search angemeldeten Benutzers, sodass Informationen unternehmensweit gemeinsam genutzt werden können, ohne die Sicherheit zu beeinträchtigen.

Borland LDAP QuickStart Manager

Verfügbar mit beiden Lizenzen.

Borland LDAP QuickStart Managerist ein Dienstprogramm, mit dem Benutzerdaten aus einem Verzeichnisdienst oder aus einer LDIF-Datei auf CaliberRM oder StarTeam-Server importiert werden können. Die importierten Benutzerinformationen werden als Benutzereigenschaften auf dem entsprechenden Server gespeichert.

StarTeam Layout-Designer

Verfügbar mit beiden Lizenzen für den Cross-Platform Client und den Web Client-Client.

Der StarTeam Layout-Designerbietet die Möglichkeit, Formulare innerhalb der Anwendung anzupassen. Mit diesen benutzerdefinierten Formularen können Sie benutzerdefinierte Eigenschaften anzeigen, Standardeigenschaften

verbergen, die für Ihr Unternehmen nicht von Interesse sind, oder die Benutzeroberfläche an die Anforderungen Ihres Unternehmens anpassen.

StarTeam Toolbar-Dienstprogramm

Die StarTeam Toolbar-Dienstprogramm, im Folgenden einfach als 'Toolbar' bezeichnet, ist eine Komponente der StarTeam- und CaliberRM-Produkte, die Ihnen das Anmelden bei mehreren Servern und das Starten mehrerer Programme erleichtert. Sie legt den Benutzernamen und das Passwort, den bzw. das Sie für die Anmeldung bei den einzelnen StarTeam- oder CaliberRM-Server verwendet haben, im Cache-Speicher ab, sodass die Anzahl der erforderlichen Anmeldungen reduziert wird. Die Toolbar wird anfänglich automatisch mit den Verknüpfungen für die Tools der auf Ihrem System installierten StarTeam- und CaliberRM-Produkte gefüllt. Da die Toolbar die standardmäßige Windows-Programmverknüpfungsfunktion verwendet, können Sie ihr problemlos weitere Programme hinzufügen.

StarTeam Datamart

Verfügbar mit Enterprise Advantage-Lizenzen. Kann separat mit Enterprise-Lizenzen erworben werden.

StarTeam Datamartist ein Ergänzungsprodukt für den StarTeam-Server. StarTeam Datamartverwendet das StarTeam SDK zu Kommunikation mit dem StarTeam-Server, um eine Berichtsdatenbank zu erstellen. Diese kann mit gängigen Berichtsanwendungen von Drittanbietern wie Crystal Reports und Business Objects verwendet werden (Berichtsanwendungen sind im Lieferumfang von StarTeam Datamartnicht enthalten). StarTeam Datamart extrahiert Daten von einem StarTeam-Server und überträgt diese in eine relationale Datenbank, auf die die Berichts-Tools zugreifen können. StarTeam Datamart kann Informationen aus allen Projekten, Projektansichten, Ordnern in Ansichten und aus allen Elementen innerhalb eines Ordners extrahieren. Dasselbe gilt für Labels, Verknüpfungen und Protokolle der Elemente. Der Extraktionsprozess kann jedoch auch auf bestimmte Projekte und Ansichten oder Tabellen beschränkt werden.

StarTeam Import/Export Manager

Verfügbar für beide Lizenzen.

StarTeam Import/Export Manager ist ein Set mehrerer Dienstprogramme, mit denen Sie ein Projekt bei Bedarf von einem StarTeam-Server auf einen anderen kopieren können.

File Compare/Merge

File Compare/Merge ist ein grafisches Tool zum Vergleichen/Zusammenführen, das zum Lieferumfang von Cross-Platform Client gehört. Es ermöglicht Ihnen, eine Datei dynamisch mit der Datei im Repository zu vergleichen und den Inhalt der beiden Dateien manuell oder automatisch zusammenzuführen. Dateiunterschiede werden unter Verwendung eines konfigurierbaren Farbschemas in den File Compare/Merge-Fenstern markiert und in den hervorgehobenen Bereichen werden Aktionsschalter angezeigt, um den Zusammenführungsprozess zu erleichtern.

View Compare/Merge

View Compare/Merge ist ein umfassendes Tool für das Vergleichen und Zusammenführen von Ansichten mit dem Cross-Platform Client. Es gibt zwei Versionen von View Compare/Merge:

- Grafisch: Bietet ein interaktives Vergleichen und Zusammenführen mit element- und ordnerspezifischer Interaktion und ermöglicht es Ihnen, sorgfältig zu steuern, welche Elemente verglichen und wie die einzelnen Unterschiede aufgelöst werden.

- Befehlszeile: Ermöglicht Batch-/Shell-gesteuerte Sitzungen.

StarTeam SDK

Das StarTeam SDK bietet die folgenden Funktionen:

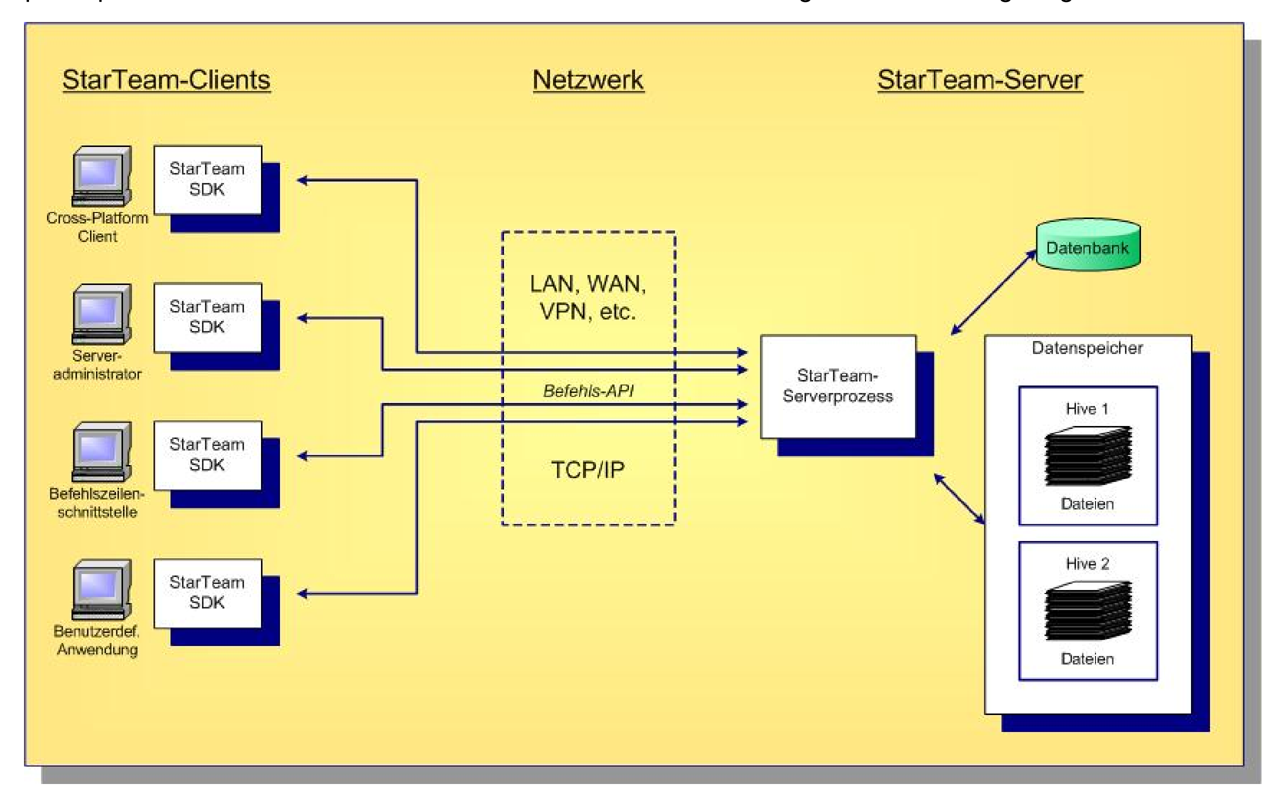
- Uneingeschränkten Zugriff auf das StarTeam-Repository zum Entwickeln benutzerdefinierter Lösungen Projektmappe oder zur Integration von Drittanbieter-Produkten
- Java-API für die Anwendungsportierbarkeit
- COM-Wrapper für die Unterstützung von Skriptsprachen über eine COM-Interface-Ebene
- Microsoft .NET Assembly unterstützt von StarTeam-COM-Objekten
- Unterstützung für die Publish/Subscribe-Technologie von StarTeamMPX

Verwandte Konzepte

Neue Funktionen in StarTeam 2009
Wo befindet sich die Dokumentation für die einzelnen Produkte
Einführung in die Benutzeroberfläche

Übersicht über die Standard-StarTeam-Architektur

Die Standard-Architektur setzt sich aus der Mindestanzahl an Komponenten für eine StarTeam-Instanz zusammen: ein StarTeam-Serverprozess, der einen Datenspeicher und eine Datenbank verwaltet, sowie ein oder mehrere StarTeam-Clients. Mit diesen Komponenten sind bereits alle wesentlichen StarTeam-Funktionen verfügbar. Die Hauptkomponenten der Standard-StarTeam-Architektur sind in der folgenden Abbildung dargestellt.



StarTeam bedient sich einer Client/Server-Architektur. *Cross-Platform-Client* (CPC), *Server Administrator* (Serveradministrations-Tool) und die *Befehlszeilenschnittstelle* sind Beispiele für im Umfang von StarTeam enthaltene Clients. StarTeam-Clients verwenden das kostenlos verfügbare *StarTeam-SDK*, daher ist es Ihnen möglich, benutzerdefinierte Anwendungen zu schreiben, die auf dieselben Funktionen zugreifen können wie die im Umfang von StarTeam enthaltenen Clients. Der vollständige Funktionsumfang des SDK kann zum Schreiben von Java-, .NET- und COM-Anwendungen verwendet werden. Ein einzelner StarTeam-Client kann mehrere Sitzungen mit einer beliebigen Anzahl an StarTeam-Servern unterhalten.

Alle StarTeam-Clients stellen mithilfe von TCP/IP eine Verbindung zum StarTeam-Serverprozess her. Daher kann praktisch jeder Netzwerktyp verwendet werden: LAN, WAN, VPN oder das öffentliche Internet. StarTeam verwendet ein proprietäres Protokoll, das als *Befehls-API* bezeichnet wird. Es unterstützt Komprimierung und mehrere Verschlüsselungsebenen. Die Befehls-API unterstützt hohe Performance, automatische Neuverbindungen, das Delta-Check-Out für langsame Verbindungen und weitere wichtige Funktionen.

Eine einzelne Bereitstellungsinstanz von StarTeam wird als *Serverkonfiguration* oder auch einfach nur *Konfiguration* bezeichnet. Die beständigen Daten einer Konfiguration sind in einer *Datenbank* und einem *Datenspeicher* enthalten und werden von einem *StarTeam-Serverprozess* verwaltet. In der Datenbank werden alle Metadaten und Artefakte gespeichert, die keine Dateien sind, Dateiinhalte werden hingegen im Datenspeicher abgelegt. Bei der Datenbank kann es sich um Microsoft SQL Server Express (SSE), einen vollständigen SQL-Server oder eine Oracle-Datenbank handeln. Sie kann auf demselben Rechner wie der StarTeam-Serverprozess oder auf einem anderen Rechner installiert sein. Die StarTeam-Datenbank und der Datenspeicher können während der Verwendung des Servers dynamisch gesichert werden. Daher ist es möglich, das System rund um die Uhr mit einem Minimum an Ausfallzeiten zu nutzen.

Der StarTeam-Datenspeicher ist eine kritische Komponente, die sich auf die Performance und Skalierbarkeit auswirkt. Im Gegensatz zur herkömmlichen *Delta-Speicherungsverfahren* verwendet der StarTeam-Datenspeicher

eine innovative (zum Patent angemeldete) Architektur, die skalierbar, leistungsfähig, hoch verfügbar und dynamisch erweiterbar ist. Derzeit speichern Kunden bis zu einem Terabyte an Daten in einem einzigen StarTeam-Datenspeicher. Dieser wurde jedoch für Daten von bis zu einem Petabyte und mehr ausgelegt.

Innerhalb des Datenspeichers werden die Dateien in Containern gespeichert, die aus als *Hives* bezeichnet werden. Ein Hive ist eine Ordnerstruktur mit *Archiv*- und *Cache*-Dateien auf einem einzigen Festplatten-Volume. Hives können dynamisch zu vorhandenen oder neuen Festplattenvolumen hinzugefügt werden. Die Kapazität ist daher praktisch unbegrenzt. StarTeam speichert jede Dateirevision in einer eigenen Archivdatei, wobei der Speicherplatzbedarf minimiert und doppelte Inhalte vermieden werden. Der StarTeam-Datenspeicher benötigt weniger Speicherplatz als Delta-Speicherungsverfahren. In bestimmten Fällen ist es von Vorteil, Datei-Deltas und keine Vollversionen an Clients zu versenden. Hierfür generiert StarTeam Delta-Dateien und legt sie im Cache-Speicher ab. In den meisten Fällen ist es jedoch günstiger, Vollversionen zu versenden.

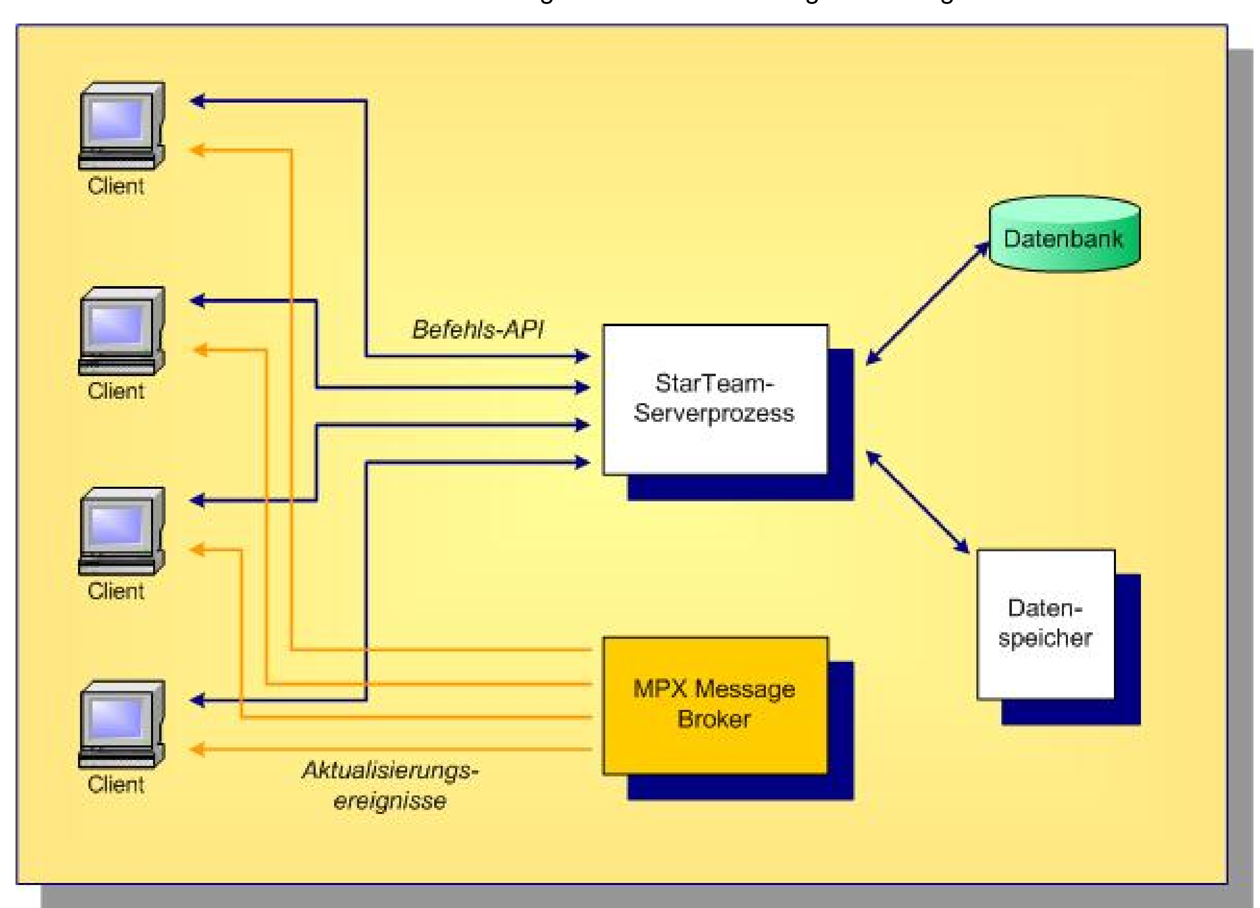
StarTeamMPX-Komponenten

Bei allen Client/Server-Architekturen mit einer wachsenden Anzahl an Clients stellen Server potentielle Engpässe dar. Die Skalierbarkeit vieler Client/Server-Systeme hängt vollständig von den Servern ab. Andere Client/Server-Systeme gewährleisten Skalierbarkeit durch die Bereitstellung mehrerer Instanzen und die Synchronisierung der Daten durch Replizierung zwischen den Instanzen.

StarTeamMPX (kurz *MPX*) ist eine einzigartige Lösung für die Skalierbarkeit von Client/Server-Systemen. MPX ist ein Publish/Subscribe-Nachrichten-Framework, das Update-Ereignisse mit Metadaten und Daten an Clients weitergibt. Es handelt sich hierbei um eine optionale Funktion, da sie nicht für die wesentlichen StarTeam-Aufgaben erforderlich ist. Ein aktiviertes MPX optimiert die StarTeam-Server-Skalierbarkeit und ermöglicht schnellere Antwortzeiten des StarTeam-Clients.

Message Broker

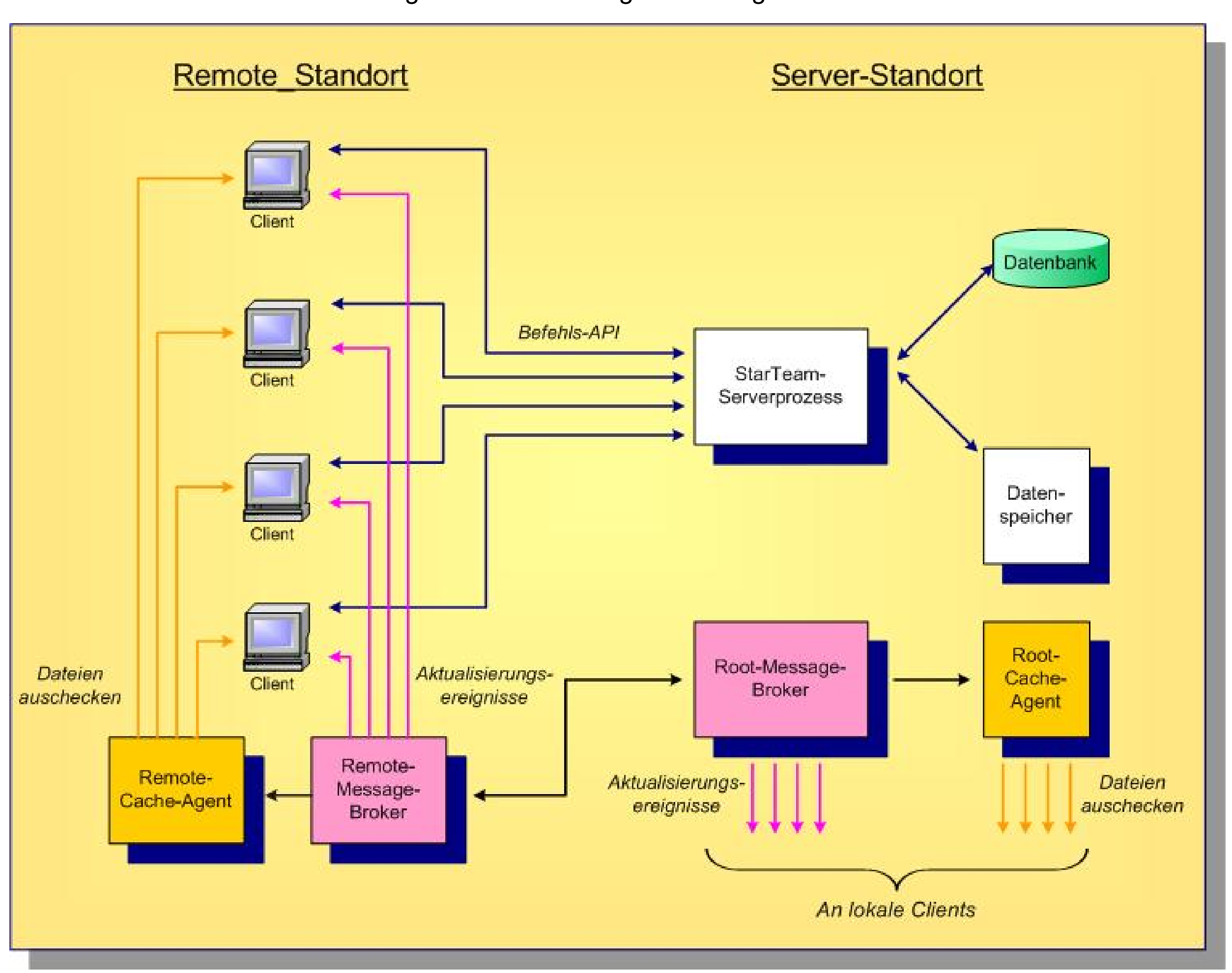
Für eine Basiskonfiguration von MPX ist eine einzelne zusätzliche Komponente erforderlich, die als *Message Broker* bezeichnet wird. Die Funktion des Message Brokers wird im Folgenden dargestellt.



Der Message Broker ist ein Messaging-Prozess, der eine *Ereignis-API* verwendet, um Aktualisierungen vom StarTeam-Serverprozess zu empfangen. Der Message Broker sendet verschlüsselte Nachrichten, die aktualisierte Artefakte enthalten. StarTeam-Clients abonnieren lediglich *Themen* und empfangen nur die relevanten Nachrichten. StarTeam-Clients empfangen vorgenommene Aktualisierungen sofort und müssen sie daher nicht abfragen oder den Cache-Speicher aktualisieren. Dies reduziert wiederum erheblich die an den StarTeam-Server gerichteten Client-Anforderungen. Außerdem wird die Server-Skalierbarkeit und die Antwortzeit der Clients optimiert, da Aktualisierungen innerhalb von Sekunden empfangen werden.

Cache-Agenten

Die vom Message Broker gesendeten Nachrichten sind nützlich für Clients mit aktiven Sitzungen. Für Dateien bietet MPX einen optionalen *Cache-Agenten*-Prozess, der einen eigenen beständigen Cache-Speicher verwaltet. Cache-Agenten können an geografischen Standorten zum Einsatz bereitgestellt werden, damit Clients Dateiinhalte vom nächsten Cache-Agenten und nicht über eine lange (und möglicherweise langsamere) Netzwerkverbindung herunterladen müssen. MPX-Cache-Agenten sind im Folgenden dargestellt.



In diesem Beispiel wird ein *Root-Cache-Agent* "netzwerknah" zum StarTeam-Serverprozess zum Einsatz bereitgestellt. Ein Root-Cache-Agent greift direkt auf den StarTeam-Datenspeicher zu, dadurch erhalten die lokalen Clients einen alternativen Pfad zum Datenspeicher für das Auschecken von Dateien. Dies reduziert die Anforderungen an den StarTeam-Server und optimiert dessen Skalierbarkeit.

Dieses Beispiel enthält außerdem einen *Remote-Message-Broker* und einen *Remote-Cache-Agenten*, die an einem entfernten Standort zum Einsatz bereitgestellt wurden. Beim *Weiterleiten von Broker zu Broker*, wird jedes Aktualisierungsereignis einmal an einen Remote-Message-Broker weitergeleitet, der es anschließend per Broadcast an die lokalen Clients versendet. Die Dateien werden an den Remote-Cache-Agenten übertragen und in einem verschlüsselten privaten Cache-Speicher abgelegt. StarTeam-Clients, die sich im Netzwerk nahe beim Remote-Cache-Agenten befinden, können jederzeit Dateien auschecken und dabei das lokale Hochgeschwindigkeitsnetzwerk nutzen, anstatt Inhalte über das WAN abzurufen. Dies wiederum reduziert die Anzahl der Anforderungen an den StarTeam-Server und optimiert die Performance der Remote-Clients.

Andere Optionen für verteilt arbeitende Organisationen

MPX bietet eine einzigartige Lösung für verteilt arbeitende Teams. Es nutzt die Vorteile eines zentralisierten Servers - niedrige Gesamtbetriebskosten, höhere Sicherheit und vereinfachte Administration - und löst die bekannten

Probleme bezüglich Performance und Skalierbarkeit von Client/Server-Architekturen. MPX bietet verteilt arbeitenden Organisationen zahlreiche Vorteile:

- Eine beliebige Anzahl an Message Brokers können miteinander zu einer "Messaging-Cloud" verkettet werden (in der Regel in einer Hub-and-Spoke-Konfiguration), die an jede beliebige Organisationsgröße anpassbar ist. Die Grenzwerte für Message Broker können frei gewählt werden und variieren je nach verfügbaren Ressourcen, z. B. Datei-Handles.
- Eine beliebige Anzahl an Cache-Agenten kann global verteilt werden. Clients können so konfiguriert werden, dass sie automatisch den Netzwerk-nächsten Cache-Agenten ermitteln und verwenden oder einen spezifischen Cache-Agenten auswählen.
- Cache-Agenten verwenden das *Push-Caching*, bei dem Inhalte nach der Erstellung mithilfe von Cache-Agenten per Broadcast versendet und gespeichert werden. Hierdurch sind Cache-Speicher effektiver als beim herkömmlichen "Pull-through"-Caching, bei dem jede erste Anforderung keine Übereinstimmungen im Cache-Speicher findet.
- Cache-Agenten verwenden erweiterte Synchronisierungstechniken, die ihre Effektivität optimieren, z. B. *Pre-Charging*, *Tiering*, *Anforderungsweiterleitung* und *automatisches Catch-up*.

Neue Funktionen in StarTeam 2009

Dieser Abschnitt bietet eine Übersicht über die neuen Funktionen in StarTeam 2009.

In diesem Abschnitt

Neue Funktionen in StarTeam 2009 Server

Diese Version des StarTeam 2009 Servers enthält die folgenden neuen Funktionen:

Online-Bereinigung

Ab StarTeam 2009 Server gibt es die Online-Bereinigung.

- Mit der Online-Bereinigung können Sie eine Datenbereinigung durchführen, während der Server läuft, was die durch Wartungstätigkeiten verursachte Ausfallzeit deutlich verringert.
- Der Prozess der Online-Bereinigung kann anhand einer neuen Ansicht für die Online-Bereinigung im Serveradministrations-Tool gestartet und gestoppt werden. Sie können zudem ein SDK-Skript zum Steuern und Automatisieren des Online-Bereinigungsprozesses erstellen. Sie können damit die Bereinigung zu bestimmten Zeiten starten und stoppen sowie verhindern, dass Daten während Spitzenlastzeiten bereinigt werden.
- Die neue Online-Bereinigung ist schneller als die vorherige Offline-Implementierung. Die Offline-Bereinigung ist in StarTeam 2009 weiterhin verfügbar, wird aber in nachfolgenden Versionen entfernt.
- Die Änderungen an der Online-Bereinigung geschieht in Phasen über mehrere Versionen hinweg. In StarTeam 2009 stehen neu gelöschte Daten nur dann zum Bereinigen zur Verfügung, nachdem ein Neustart des Servers durchgeführt wurde.
- Die Online-Bereinigung ist ein interaktiver Prozess, der jederzeit gestartet und gestoppt werden kann, solange der Server läuft. Die Online-Bereinigung zeichnet ihren aktuellen Ausführungsstatus auf und kann exakt von dem Punkt aus neu gestartet werden, an dem sie gestoppt wurde. Nach einem Neustart des Servers muss die Online-Bereinigung manuell neu gestartet werden.
- Sie können die Online-Bereinigung sowohl auf einem Remote-Server als auch auf einem lokalen Server starten und stoppen.

StarTeam-Verbindungssteuerung

StarTeam 2009 Server ermöglicht Administratoren, die Client-Anwendungen zu optimieren, die eine Verbindung zum Server aufnehmen können, indem Sie eine neue `app-control.xml`-Datei anpassen. Diese Funktion verhindert, dass unerwünschte SDK-Anwendungen eine Verbindung zum Server herstellen und Serverressourcen binden.

Hinweis: Dies ist grundsätzlich eine administrative, aber keine Sicherheitsmaßnahme.

Konfigurationsdatei "app-control.xml"

Der Server sucht nach einer neuen Konfigurationsdatei mit dem Namen **app-control.xml**, die sich im Unterverzeichnis `AppControl` unter dem Stammverzeichnis des StarTeam-Repositorys befindet. Wenn eine neue Konfiguration erstellt wird, erzeugt StarTeam 2009 Server diese Datei aus der Vorlage `app-control.xml`, die sich im Verzeichnis `AppControl` unter dem Server-Installationsverzeichnis befindet.

Die Konfigurationsdatei `app-control.xml` enthält, falls vorhanden, einen Regelsatz. Jede Regel weist den Server an, die eingehenden Client-Verbindungen zu testen, um sicherzustellen, dass eine oder mehrere der folgenden Bedingungen erfüllt sind:

- Das StarTeam SDK ist neuer oder gleich einer bestimmten Version.
- Der Anwendungsname, der Name des verbindenden Benutzers und/oder der Client-Workstation-Name müssen mit einem angegebenen Textmuster übereinstimmen.

Der Server testet jede eingehende Client-Verbindung anhand der Regeln in der Datei `app-control.xml`, bis eine Übereinstimmung gefunden wird oder die Regelliste abgearbeitet ist. Sobald eine Übereinstimmung gefunden wird, werden keine weiteren Prüfungen mehr durchgeführt und die Sequenz für das Verbindungs-Handshake wird fortgesetzt. Wird keine Übereinstimmung gefunden, wird die Verbindung verweigert. Wenn die Datei `app-control.xml` nicht im Verzeichnis `AppControl` vorhanden ist, erlaubt der Server allen unterstützten Client-Anwendungen, eine Verbindung herzustellen.

AllowedApp

`AllowedApp:` Dies ist das Haupt-Regelelement. Es muss ein `Namensattribut` haben, das das Textmuster für den Namen der Client-Anwendung angibt (wie z. B. "Client-Identifikations-String"). Das Textmuster kann ein Sternchen ("*") als Platzhalter enthalten. Neben dem `Namensattribut` kann dieser Knoten optional ein oder mehrere der folgenden Attribute angeben:

- `MinimumSDKVersion:` gibt die Mindestversion des StarTeam SDK an, mit der die Client-Anwendung gebaut wird. Das Format dieses Felds ist `nn.nn.nn.nn`, wobei `nn` eine nicht-negative Zahl ist. Es müssen nicht alle Punktnummern angegeben werden, beispielsweise lässt `MinimumSDKVersion="10.4"` die Versionen `10.4.x.y` und höher (`10.5`, `11.0` usw.) zu.
- `WorkStationID:` Falls festgelegt, wird damit das Textmuster für den Namen des Client-Computers angegeben.
- `Name:` Falls festgelegt, wird damit das Textmuster für den StarTeam-Benutzernamen angegeben.

Wenn kein optionaler Parameter gesetzt ist, testet der Server das entsprechende Verbindungsattribut nicht.

AppDefault

`AppDefault:` Dies ist ein optionales Element, das zum Angeben der Standardwerte für einen der Parameter verwendet werden kann, die unter `AllowedApp` aufgelistet sind. Die Syntax dieses Elements entspricht der Syntax für `AllowedApp` mit der Ausnahme, dass das `Namensattribut` keinen Standardwert haben kann. Für `MinimumSDKVersion`, `WorkStationID` und `UserName` können Standardwerte angegeben werden.

Weitere Funktionen von StarTeam 2009 Server

Diese Version des Servers enthält zusätzlich die folgenden neuen Funktionen:

- StarTeam Server für Windows wird nun für die 64-Bit-Architektur unterstützt, wodurch auf mehr verfügbaren Arbeitsspeicher zugegriffen werden kann. Dazu ist Windows Server 2008 64-Bit erforderlich.
- StarTeam Server 2009 unterstützt auch alle anderen neuen StarTeam 2009-Funktionen, wie z. B. Änderungspakete und Trace-Unterstützung für Artefakt-zu-Artefakt-Verknüpfungen (externe Links) über verschiedene Server hinweg.
- Beim Erstellen von neuen Projekten wählt StarTeam Server 2009 jetzt als Standard für neue Ansichten nur den Elementtyp "Datei" vorab aus. Benutzer können die Projekteigenschaften nach wie vor nach Erstellen des Projekts ändern und sie können auch die aufgenommenen Elementtypen für eine neue Ansicht ändern. Wenn allerdings der Benutzer nichts ändert, enthalten neue Ansichten nur dann standardmäßig Dateien, wenn sie erstellt werden. **Hinweis:** Diese Änderung wirkt sich nicht auf vorhandene Projekte aus. Sie betrifft nur neue Projekte, die mit StarTeam Server 2009 oder vorhandenen Servern, die auf StarTeam Server 2009 aktualisiert wurden, erstellt wurden. Durch das Hinzufügen von anderen Elementtypen zu den Projekteigenschaften (nachdem die Ansicht erstellt wurde) wird die Ansicht NICHT mit den Elementen gefüllt, die in der übergeordneten Ansicht enthalten waren (aber während des Erstellens der neuen Ansicht übergangen wurden). Falls der Benutzer die vorherigen Elemente in die neue Ansicht aufnehmen möchte, muss er sie abrufen, indem er die Basis von der übergeordneten Ansicht ändert.
- StarTeam Server 2009 bietet eine verbesserte Befehlsverarbeitung durch asynchrone E/A, um Lese- und Schreibvorgänge im Netzwerk auf unterstützten Windows 32-Bit- und 64-Bit-Plattformen durchzuführen. Dies

ist die zweite Phase der asynchronen E/A-Unterstützung. Die erste Phase wurde in StarTeam Server 2008 R2 implementiert und bot lediglich Unterstützung für Schreibvorgänge.

- Es gibt nun den neuen StarTeam Web Server, der den in StarTeam 2009 neu eingeführten Web-Client unterstützt.
- Es wurden zusätzliche Änderungen vorgenommen, um die Serverleistung zu verbessern.
- Die Installationsanweisungen für den Linux-Server wurden in das "StarTeam 2009-Installationshandbuch" (`ST_Install_en.pdf`) verschoben, das unter http://techpubs.borland.com/starteam/ zur Verfügung steht.
- Das StarTeam Serveradministrations-Tool verwendet die neue Eclipse-Infocenter-Hilfe. Weitere Informationen hierzu finden Sie unter "Neues in der Dokumentation" in "Neue Funktionen in anderen StarTeam 2009-Komponenten und -Produkten".

Neue Funktionen im StarTeam 2009-Cross-Platform-Client

Dieses Thema beschreibt die neuen Funktionen und Änderungen in dieser Version des StarTeam 2009 Cross-Platform Client.

Die folgenden neuen Funktionen in dieser Version werden in den nachfolgenden Abschnitten näher beschrieben:

- Änderungspakete
- Externe Links
- EOL-Verbesserungen
- Weitere Änderungen am Cross-Platform-Client

Änderungspakete

StarTeam hat bisher viele Funktionen bereitgestellt, die das Änderungsmanagement (CM) einschließlich integrierter Workflows, benutzerdefinierbarer Workflows, Prozess-Links, Prozess-Tasks und des Vergleichens/ Zusammenführens von Ansichten (VCM) unterstützt. Mit StarTeam 2009 gibt es jetzt eine umfassende *Änderungspaket*-Funktion, die es Ihnen ermöglicht, unter Verwendung eines Änderungspaketobjekts alle in einem einzelnen Festschreibevorgang vorgenommenen Änderungen aufzuzeichnen. Dank dieser neuen Funktion verwendet VCM jetzt Änderungspakets anstelle von VCM-Prozess-Tasks. Bei Änderungspaketen handelt es sich um eine Änderungsmanagementfunktion, die es StarTeam ermöglicht, Änderungen besser zu verwalten und aufzuzeichnen. Änderungspakete sind eine Weiterentwicklung der VCM-Funktion, die erstmalig in StarTeam 2006 eingeführt wurden.

Weitere Informationen zur neuen Änderungspaketfunktion finden Sie unter "Neue Funktionen in View Compare/ Merge (VCM)".

Externe Links

Mithilfe der neuen Funktion für externe Links ist es jetzt möglich, Elemente auf verschiedenen Servern zu verknüpfen (Element-zu-Element-Links über Server hinweg). Das Erstellen von externen Links ist im Grunde genommen dem Erstellen von Links zwischen Elementen auf demselben Server ähnlich. Ein externer Link hat jedoch eine Dekoration ( ), der deutlich anzeigt, dass es sich um einen externen Link und nicht um einen normalen Link handelt. Außerdem gibt es ein neues Auswahlfeld auf dem Register "Link", mit dem Sie externe Links anzeigen oder verbergen können.

- Die gleichen Link-Operationen stehen sowohl für externe als auch für normale Links zur Verfügung, z. B. Link erstellen, Link abschließen und Drag-and-Drop-Operationen. Die Projekte auf beiden Servern, die die Elemente enthalten, die Sie verknüpfen möchten, müssen gleichzeitig im Cross-Platform-Client geöffnet werden, um externe Links zu erstellen.
- Im Fenster "Links" können Sie auch nach externen Links in allen Servern suchen, bei denen Sie angemeldet sind.
- Wenn Sie einen externen Link erstellen, werden im Fenster "Links" die Elementdetails für den externen Link durch eine URL angegeben, damit Sie das Element finden können
- Die Optionen für externe Links sind die gleichen wie für normalen Links, z. B. haben Sie die Möglichkeit, Link-Eigenschaften anzuzeigen. Frei platzierbare und angeheftete externe Links stehen allerdings nicht zur Verfügung.
- Externe Links weisen eine Richtung auf. Ob Sie die externen Links vom Quellelement des Links, z. B. einer Änderungsanforderung, oder von dem Element auf dem externen Server, z. B. der Datei, die als Linkziel der Änderungsanforderung dient, aus betrachten, die Quell- und Zielinformationen bleiben immer gleich, d. h. sie hängen nicht vom ausgewählten Element ab.

- Sie können externe Links nur mit Objekten erstellen, die auf einem StarTeam-Server der Version 2009 vorhanden sind, der externe Links unterstützt. Hierzu muss der Cross-Platform-Client von StarTeam 2009 verwendet werden. Nur das Quellelement des externen Links muss sich auf einem StarTeam-Server der Version 2009 befinden.
- Sie können keine externen Links mit oder zwischen Änderungspaketen erstellen.
- Einige Informationen, die für normale Links vorhanden sind, stehen nicht für externe Links nicht zur Verfügung, weil nicht alle Informationen aus dem externen Objekt verfügbar sind, z. B. der Dateistatus, wer die Datei auf dem externen Server gesperrt hat, der Ordnerpfad des Objekts und der Ordner, in dem sich das Objekt tatsächlich befindet.
- Dialogfelder des Typs **Zugriffsrechte** enthalten jetzt die Zugriffsrechte für **Externe Links** auf Containerebene.

EOL-Verbesserungen

EOL-Verbesserungen sorgen für eine verbesserte Unterstützung von Dateien mit fester EOL-Konvertierung. Beispielsweise funktioniert die EOL-Konvertierung nun ordnungsgemäß für Unicode-Dateien, die zuvor beim Einchecken beschädigt werden konnten.

Dateien können auf jeder Plattform und ungeachtet spezifischer Optionen im LF-Format ausgecheckt werden. Darüber hinaus funktioniert "Status aktualisieren" für alle Textdateien, nachdem das EOL-Format definiert wurde und ungeachtet des EOL-Formats, das verwendet wurde, als sie ausgecheckt wurden.

Aus Kompatibilitätsgründen mit älteren Clients werden Dateien, bei denen "EOL-Konvertierung" beim Auschecken nicht angefordert wird und das EOL-Format nicht definiert ist, mit derselben EOL-Konvertierung ausgecheckt, mit der sie zum Server hinzugefügt wurden.

StarTeam 2009 bietet die folgende neue EOL-Handhabung.

- Die Eigenschaft wird noch als "EOL-Zeichen" im Elementefenster des Cross-Platform-Clients angezeigt.
- Die Eigenschaft "EOL-Format" ist nur sinnvoll für Textdateien während des Auscheckvorgangs.
- Die EOL-Eigenschaftswerte sind:
  - *Nicht definiert* (null im SDK): Wird für Dateien verwendet, die vor StarTeam 2009 hinzugefügt wurden.
  - *Von Client bestimmt*: Sorgt dafür, dass die EOL-Konvertierung pro Auscheckvorgang oder die Standard-Workstation-Konvertierung verwendet wird.
  - *Festes CR*, *Festes LF* und *Festes CRLF*: Bewirkt, dass dieses EOL-Format immer angewendet wird. Die Workstation-/Auscheck-Konvertierungsoption wird ignoriert.

- Die Eigenschaft "EOL-Format" kann in den Dialogfeldern **Hinzufügen/Einchecken** und **Dateieigenschaften** des Cross-Platform-Clients festgelegt werden.
- Die EOL-Konvertierung des Cross-Platform-Clients für die Hinzufügen/Einchecken-Optionen wurden entfernt.
- Unter den folgenden Bedingungen ermittelt das SDK standardmäßig das EOL-Format:
  - Wenn eine neue Textdatei hinzugefügt oder eine neue Revision für eine Textdatei eingecheckt wird, deren EOL-Format *Nicht definiert* ist, und die EOL-Konvention der Datei mit der Standardkonvention der Plattform übereinstimmt, wird das EOL-Format auf *Von Client bestimmt* festgelegt. Anderenfalls wird das EOL-Format auf die Konvention festgelegt, die gefunden wurde: *Festes LF*, *Festes CR* oder *Festes CRLF*.
  - Der Benutzer kann jederzeit das EOL-Format in einen anderen Wert ändern (außer *Nicht definiert*).

- Ungeachtet der EOL-Format-Einstellung verwenden Textdateien, die mithilfe eines StarTeam 2009 Cross-Platform-Clients hinzugefügt oder eingecheckt werden, immer ein kanonisches Format (CRLF) im Datenspeicher.

Hinweis: Der Standard für die automatische EOL-Konvertierung für die Operation zum Auschecken wurde in "markiert" geändert, wenn der Benutzer diese Option nicht bereits definiert hat. Benutzer, die auf 2009 aktualisieren, sollten diese Option überprüfen, um sicherzustellen, dass Sie sie vor dem Hintergrund der neuen EOL-Formatänderungen korrekt eingestellt haben.

Weitere neue Funktionen des Cross-Platform-Clients

Im Folgenden sind zusätzliche neue Funktionen des Cross-Platform-Clients aufgeführt:

- StarTeam 2009 bietet jetzt so genannte "Me"-Abfragen, die ermöglichen, dass eine Abfrage eingerichtet werden kann, die auf Basis des aktuell angemeldeten Benutzers ("Me") ausgewertet wird. Somit muss beim Erstellen der Abfrage kein Benutzername mehr angegeben werden.
- Die Reihenfolge des Kontextmenüs für **Ordner** wurde geändert. Um die Konsistenz zu verbessern, ähnelt es jetzt mehr dem Kontextmenü für **Elementtabellen**.
- Das Dialogfeld **Ansicht auswählen** bietet ein neues Auswahlfeld, das es dem Benutzer ermöglicht, die ausgewählte Ansicht in einem neuen Ansichtsfenster zu öffnen.
- Ordnersymbole im Ordnerbaum haben einen neuen Dekorator, um anzugeben, dass statt des Standardarbeitspfads ein Ordner einen alternativen Pfad für den Arbeitsordner verwendet.
- Beim Erstellen eines neuen Projekts hat der Server bisher eine Vorauswahl aller Elementtypen für die Projekteigenschaften getroffen. Dies führte dazu, dass, wenn der Benutzer im Dialogfeld **Projekteigenschaften** oder im **Assistent für neue Ansicht** nichts änderte, neue Ansichten alle Elementtypen erhielten. Es wird daher empfohlen, bei neuen Ansichten nur den Elementtyp **Datei** zu verwenden. Beim Erstellen von neuen Projekten wählt StarTeam Server 2009 jetzt als Standard für neue Ansichten nur den Elementtyp **Datei** vorab aus. Benutzer können die Projekteigenschaften nach wie vor nach Erstellen des Projekts ändern und sie können auch die aufgenommenen Elementtypen für eine neue Ansicht ändern. Wenn allerdings der Benutzer nichts ändert, enthalten neue Ansichten nur dann standardmäßig Dateien, wenn sie erstellt werden. Diese Änderung wirkt sich nicht auf vorhandene Projekte aus. Sie betrifft nur neue Projekte, die mit StarTeam Server 2009 oder vorhandenen Servern, die auf StarTeam Server 2009 aktualisiert wurden, erstellt wurden. **Hinweis:** Durch das Hinzufügen von anderen Elementtypen zu den Projekteigenschaften (nachdem die Ansicht erstellt wurde) wird die Ansicht NICHT mit den Elementen gefüllt, die in der übergeordneten Ansicht enthalten waren (aber während des Erstellens der neuen Ansicht übergangen wurden). Falls der Benutzer die vorherigen Elemente in die neue Ansicht aufnehmen möchte, muss er sie abrufen, indem er mit View Compare/Merge eine Neubestimmung der Basis von der übergeordneten Ansicht vornimmt.
- Der Cross-Platform-Client unterstützt nun den Vergleich von Eigenschaften von Nicht-Datei-Elementen unter Verwendung des eingebetteten Vergleichsfensters. Sie können beispielsweise im Elementefenster zwei Änderungsanforderungen oder zwei historische Revisionen derselben Änderungsanforderung auswählen und **Tools** ▸ **Vergleichen** wählen, um deren Eigenschaften zu vergleichen. Das eingebettete Vergleichsfenster wird unten im Fenster angezeigt und enthält die Eigenschaften der ausgewählten Änderungsanforderungen. Diese neue Funktion betrifft die Register **Element** und **Information** sowohl in der **Inhaltsperspektive** als auch in der **Änderungsperspektive**.
- Das Dialogfeld zum **Einchecken von Dateien** zeigt keine eingefrorenen Revisions-Labels mehr an.

Neue Funktionen beim Vergleichen/Zusammenführen von Ansichten (View Compare/Merge, VCM)

In diesem Thema werden die Änderungen und neuen Funktionen beim Vergleichen/Zusammenführen von Ansichten und des VCM-Dienstprogramms beschrieben.

Änderungspakete

StarTeam hat bisher viele Funktionen bereitgestellt, die das Änderungsmanagement (CM) einschließlich integrierter Workflows, benutzerdefinierbarer Workflows, Prozess-Links, Prozess-Tasks und des Vergleichens/ Zusammenführens von Ansichten (VCM) unterstützen. Mit StarTeam 2009 gibt es jetzt ein umfassendes *Änderungspaketobjekt*, das es Ihnen ermöglicht, alle in einem einzelnen Festschreibevorgang vorgenommenen Änderungen aufzuzeichnen. Dank dieser neuen Funktion erstellt VCM jetzt Änderungspakete anstelle von VCM-Prozess-Tasks.

Änderungspakete verbessern die Fähigkeit von StarTeam, Aktualisierungen zu verwalten und aufzuzeichnen. Änderungspakete sind eine Weiterentwicklung der VCM-Funktion, die erstmalig in StarTeam 2006 eingeführt wurden. Ein Änderungspaket ist ein Objekt, das die an einer Zielansicht vorgenommenen Änderungen enthält. Um ein Änderungspaket zu erstellen, muss ein Benutzer zuerst eine VCM-Sitzung starten, die als Staging-Bereich fungiert, in dem Änderungen definiert, überarbeitet und getestet werden.

Eine VCM-Sitzung ist in der Zielansicht als ein Änderungspaket sichtbar, nachdem es gespeichert oder festgeschrieben wurde.

- Als Ergebnis der Verwendung des neuen Änderungspaketelements werden Zusammenführungspunkte und Prozess-Tasks in VCM-Sitzungen zum Aufzeichnen von Änderungen nicht mehr verwendet.
- Das StarTeam-Ansichtsfenster enthält nun Perspektiven. Per Klick auf ein Symbol können Sie nun wechseln zwischen der standardmäßigen **Inhaltsperspektive**, repräsentiert durch das StarTeam-Logo, und der **Änderungsperspektive**, repräsentiert durch ein neues Symbol neben dem standardmäßigen Symbol. Diese neuen Perspektivsymbole sind in der Symbolleiste rechtsbündig angeordnet. Ein Manager kann beispielsweise durch Verwenden der **Änderungsperspektive** alle Änderungspaketobjekte und Details zu diesen Änderungspaketen überprüfen, sehen, welche Änderungen in einer Ansicht festgeschrieben wurden, und Änderungen in nicht festgeschriebenen Änderungspaketen, die zum Festschreiben vorgeschlagen sind, überarbeiten.
- Die Menüeinträge für VCM-Sitzungen wurden geändert. Da beispielsweise das Änderungspaket ein Objekt ist, gibt es den neuen Menüeintrag **Änderungspaket** ▸ **Eigenschaften**, um das Änderungspaket zum Anzeigen und/oder Ändern seiner Eigenschaften, wie z. B. den Arbeitsordner für die VCM-Sitzung, zu öffnen. Weitere Menüänderungen sind der Menüeintrag **Änderungspaket** ▸ **Speichern**, mit dem ein Änderungspaketobjekt in nicht festgeschriebenem Zustand in einer Zielansicht des StarTeam-Servers gespeichert wird. **Änderungspaket** ▸ **Exportieren** wird weiterhin als Möglichkeit unterstützt, eine VCM-Sitzung als `.vcmx`-Datei zu speichern, um zur Überarbeitung an andere Benutzer gesendet zu werden, obwohl Änderungspakete nun vor `.vcmx`-Dateien bevorzugt werden. Weitere Informationen zum neuen **Änderungspaket**-Menü finden Sie unter dem Thema zur Benutzeroberfläche der Änderungsperspektive in der “Einführung” unter “Einführung in die Benutzeroberfläche”.
- Da jedes Änderungspaket ein neues Objekt in StarTeam ist, das eine Gruppe von Änderungen repräsentiert, wurde in StarTeam 2009 das neue Register **Ändern** im unteren Bereich des Clients hinzugefügt. Dadurch wird das Anzeigen von durch das Änderungspaket hervorgerufenen Aktualisierungen zu einem ausgewählten Element unterstützt. Eine ausführlichere Erläuterung aller Teile der **Änderungsperspektive** ist im Abschnitt "Einführung in die Benutzeroberfläche" unter "Einführung" in der StarTeam-Hilfe verfügbar.
- In der **Änderungsperspektive** sind weitere Optionen verfügbar, wie z. B. Symbolleistenschalter, ein Standard-**Filter**-Menü und der Symbolleistenschalter zum **Ändern des Layouts**, mit dem Sie zwischen einen Links/Rechts-Layout oder einem Oben/Unten-Layout wechseln können. Im Links/Rechts-Layout werden Symbole dazu verwendet, in der **Änderungsperspektive** zwischen den Fenstern **Detail**, **Historie**,

Beschriftung, **Ändern** und **Wiederholung** zu wechseln. Im Oben/Unten-Layout können Sie mit den unteren Registern diese Ansichten ändern.

- Anhand eines Kontextmenüelements können Sie nun URLs von gespeicherten Änderungspaketen in die Zwischenablage kopieren, damit andere Benutzer die URL in der Zielansicht öffnen und das Änderungspaket im schreibgeschützten Modus anzeigen können. Das Senden einer `.vmx`-Datei mit dem Inhalt der gesamten VCM-Sitzung ist nicht mehr erforderlich.
- In der **Wiederholungsansicht** können Sie ein Änderungspaket mit Drag-and-Drop in einer anderen Ansicht wiederholen. Sie können zudem das Änderungspaket in einer VCM-Sitzung mit der Menüoption **Erweitert ▸ Ansichten vergleichen/zusammenführen** erneut öffnen, um eine **Wiederholung** in einer anderen Ansicht zu starten.
- Sie können ein Änderungspaket löschen, falls es noch nicht festgeschrieben wurde. Sobald es festgeschrieben ist, steht der Löschvorgang nicht mehr zur Verfügung.
- Sie können nicht festgeschriebene Änderungspakete exklusiv sperren. Es kann nur jeweils eine Person Änderungen an einem Änderungspaket vornehmen. Folglich wird ein Änderungspaket automatisch gesperrt, wenn es zum Bearbeiten geöffnet wird.
- Der Menübefehl **Sitzung neu starten** in der **Änderungsperspektive** ermöglicht es einem Benutzer, ein Änderungspaket in einer VCM-Sitzung neu zu starten (neu zu vergleichen).
- Das Menü für VCM-Sitzungen verfügt nun über zwei neue Befehle: **URL in die Zwischenablage kopieren** und **In Ansicht auswählen**. Wenn die aktuelle VCM-Sitzung als Änderungspaket gespeichert wurde, ermöglichen diese Befehle den einfacheren Zugriff auf gespeicherte Änderungspakete.
- Ein neues **Berichtsmenü** für Änderungspakete ist über das Dialogfeld **Berichte** verfügbar.
- Die **Änderungsperspektive** unterstützt das Menü **Eigenschaften vergleichen** zum Vergleichen der Änderungspaketeigenschaften.

Weitere VCM-Änderungen

Neben den bereits erwähnten Änderungspaketen und externen Links gibt es diese weiteren neuen Funktionen in View Compare/Merge:

- Der Experte **Ansichten vergleichen/zusammenführen** hat die neue Seite **Eigenschaften ausschließen**, auf der Sie Eigenschaften jedes verzweigbaren Elementtyps ausschließen können. Auf der Seite können Sie bestimmte Elementtypeigenschaften auswählen, für die Sie die Änderungen nicht zusammenführen möchten, wenn die Sitzung festgeschrieben wird.
- Der Experte **Ansichten vergleichen/zusammenführen** verfügt über einen neuen Schalter unten rechts auf jeder Expertenseite, mit dem ein Informationsfenster geöffnet werden kann, das Ihnen die Details zu der Auswahl anzeigt, die Sie für die VCM-Sitzung im Experten **Ansichten vergleichen/zusammenführen** bis zu diesem Schritt vorgenommen haben. Klicken Sie erneut auf den Schalter, um das Informationsfenster zu verbergen. Der Vorteil dieses Informationsfensters liegt darin, dass Sie an einer Stelle alle Details der Sitzung überprüfen können, bevor Sie auf **Fertig stellen** klicken, ohne zwischen den verschiedenen Seiten des Experten hin und her wechseln zu müssen, um zu sehen, was Sie ausgewählt haben. Wenn Sie eine Auswahl ändern möchten, können Sie zu der gewünschten Seite des Experten wechseln, die Änderung vornehmen und anschließend auf **Fertig stellen** klicken.
- Die Schalter für die **Vergleichs-**, **Zusammenführungs-** und **Testperspektive** wurden auf die rechte Seite der Symbolleiste verschoben.

Zusammenführungspunkte

Durch die Implementierung der Änderungspakete werden Zusammenführungspunkte in VCM-Sitzungen nicht mehr verwendet. VCM verwendet nun interne "Änderungsobjekte", die im Vergleich zu Zusammenführungspunkten verbesserte Zusammenführungsfunktionen liefern.

Neue oder geänderte Unterschiedstypen

Es wurden die folgenden Änderungen an Unterschiedstypen und -aktionen vorgenommen:

- *Fehlschlag* wurde geändert in *Überarbeitung erforderlich*. *Überarbeitung erforderlich* ist nun in allen Fällen eine zulässige Aktion.
- Benutzerdefinierte Zusammenführungstypen: Das Ändern der Standardaktion eines beliebigen Unterschiedstyps in *Überarbeitung erforderlich* bedeutet, dass ein Eingreifen des Benutzers erforderlich ist, bevor ein Festschreibevorgang durchgeführt werden kann.
- Bei *Als gelöst markieren* wird kein Zusammenführungspunkt mehr erstellt. Nun bedeutet es: Erstelle ein Änderungsobjekt des Typs *Als gelöst markieren*. *Als gelöst markieren* ist nun in vielen Fällen eine gültige Aktion, wo sie zuvor nicht zulässig war. Dies betrifft etwa zwei Dutzend Unterschiedstypen.
- Die Unterschiedstypen, denen keine Beachtung geschenkt werden musste, wurden repariert. Es wird nun zwischen den Fällen *In Ziel geändert* und *In Ziel nicht geändert* unterschieden.

Beispiel für StarTeam 2008 Release 2:

[2000]: In Quelle verschoben, Ziel auf anderem Zweig

```
    ItemPresentInSource: true.
    ItemPresentInTarget: true.
    ItemDeletedInSource: false.
    ItemDeletedInTarget: false.
    ItemModifiedInSource: false.
    ItemModifiedInTarget: Wurde keine Beachtung geschenkt.
    ItemMovedInSource: true.
    ItemMovedInTarget: false.
    ItemsInDifferentBranches: true
    Standardaktion: Ignorieren.
    Zulässige Aktionen: Ignorieren; Verschieben; Verschieben und überschreiben
```

Beispiel für StarTeam 2009:

[2000]: In Quelle verschoben, Ziel auf anderem Zweig

```
    ItemPresentInSource: true.
    ItemPresentInTarget: true.
    ItemDeletedInSource: false.
    ItemDeletedInTarget: false.
    ItemModifiedInSource: false.
    ItemModifiedInTarget: false.
    ItemMovedInSource: true.
    ItemMovedInTarget: false.
    ItemsInDifferentBranches: true
    Standardaktion: Ignorieren.
    Zulässige Aktionen: Ignorieren, Verschieben; Überarbeitung erforderlich, Als gelöst
markieren
```

Alte Zeilen, die nun **In Ziel geändert=false** haben

```
[2000]: In Quelle verschoben, Ziel auf anderem Zweig
[2500]: In Quelle verschoben und geändert, Ziel in anderem Zweig
[2510]: In Quelle verschoben und geändert, Ziel in anderem Zweig, Gleicher Inhalt.
```

Neue Zeilen mit **In Ziel geändert=true**

```
[2060]: In Quelle verschoben, Verzweigt und in Ziel geändert
[2520]: In Quelle verschoben und geändert, Ziel in anderem Zweig, In Ziel geändert
[2530]: In Quelle verschoben und geändert, Ziel in anderem Zweig, In Ziel geändert,Gleicher
Inhalt
```

Änderungen an der VCM-Tabelle der Aktionsentscheidungen

Die folgenden Änderungen wurden an der VCM-Tabelle der Aktionsentscheidungen für StarTeam 2009 vorgenommen:

```
[100]: Übergeordneter Ordner fehlgeschlagen

    ParentFolderFailed: true

    Standardaktion: Überarbeitung erforderlich
    Zulässige Aktionen: Ignorieren, Überarbeitung erforderlich

[110]: Übergeordneter Ordner ignoriert

    ParentFolderIgnored: true

    Standardaktion: Ignorieren
    Zulässige Aktionen: Ignorieren, Überarbeitung erforderlich

[200]: Zielordner hat unverankerte Freigabe in Quellansicht

    TargetFolderHasFloatingShares: true

    Standardaktion: Überarbeitung erforderlich
    Zulässige Aktionen: Ignorieren, Überarbeitung erforderlich

[620]: In Ziel gelöscht (Heraufstufen)

    Zusammenführungstyp: Heraufstufen
    ItemPresentInSource: true
    ItemPresentInTarget: false
    ItemDeletedInSource: false
    ItemDeletedInTarget: true

    Standardaktion: Ignorieren
    Zulässige Aktionen: Ignorieren, Freigeben, Umgekehrte Freigabe, Überarbeitung
erforderlich

[600]: In Ziel gelöscht

    ItemPresentInSource: true
    ItemPresentInTarget: false
    ItemDeletedInSource: false
    ItemDeletedInTarget: true

    Standardaktion: Ignorieren
```

```
    Zulässige Aktionen: Ignorieren, Freigeben, Überarbeitung erforderlich

[520]: Neu in Quelle, Gemeinsam genutzt (Heraufstufen)

    Zusammenführungstyp: Heraufstufen
    ItemPresentInSource: true
    ItemPresentInTarget: false
    ItemDeletedInSource: false
    SourceItemOnRootBranch: false

    Standardaktion: Überarbeitung erforderlich
    Zulässige Aktionen: Ignorieren, Freigeben, Überarbeitung erforderlich

[510]: Neu in Quelle (Heraufstufen)
```

Änderungen im Auflösen von Prozess-Tasks

Auflösen eines Prozess-Tasks in 2008 Release 2,

- Sie mussten den Prozess-Links folgen.
- Die Prozess-Links konnten ein gelöschtes Element nicht referenzieren
- Sie konnten keine *Löschvorgänge* unter Verwendung des Prozesselementbereichs weiterleiten.

Zum Auflösen eines Prozess-Tasks in 2009 gehört Folgendes:

- Das Öffnen der zugeordneten `*.vcmx`-Datei.
- Das Verwenden von *ItemDifferences* zum Ermitteln des Umfangs

Dies entspricht der Verwendung von Änderungspaket-/Änderungsobjekten.

VCMUtility - Änderungen an der Befehlszeile

VCMUTILITY ist mit Änderungspaketobjekten integriert. Es gibt neue Befehle und Sitzungsoptionen, die Änderungspakete unterstützen.

Der VCMUTILITY-Befehl wurde um die folgenden Optionen erweitert, um Änderungspakete zu unterstützen:

Befehlsoptionen

- `{Open <Name des Änderungspakets>}`
- `{Replay <Name des Änderungspakets>}`

Sitzungsoptionen

- `{Description <Beschreibung>}`
- `{Name <Name des Änderungspakets>}`

Weitere Syntaxoptionen

- `<Name des Änderungspakets>`
- `<Ordnerpfad>`
- `<VCM-Austauschdatei>`

- `<VCM-Sitzungsdatei>`

Diese und alle weiteren `VCMUtility`-Befehle und -Optionen sind im Referenzabschnitt für das Vergleichen/ Zusammenführen der Cross-Platform-Client-Hilfe aufgelistet.

Borland StarTeam 2009 Web Client

Der neue Borland® StarTeam® Web Client ist eine intuitive, webbasierte Schnittstelle, über die sich mehrere Benutzer gleichzeitig bei einem oder mehreren StarTeam-Servern anmelden sowie auf Projekte zugreifen und Elemente verwalten können.

Diese erste Version des Web-Clients enthält Kernfunktionen, die speziell auf Benutzer abgestimmt sind, die StarTeam-Änderungsanforderungen, -Anforderungen, -Tasks und -Themen anzeigen, erstellen und bearbeiten müssen.

Web-Client-Funktionen

StarTeam Web Client unterstützt die folgenden Aktivitäten:

- Öffentliche Filter auf den StarTeam Server zum Definieren des Gültigkeitsbereichs der durchzusuchenden Elemente verwenden
- Elemente erstellen, die keine Dateien sind
- Elementeigenschaften ändern
- Element sperren und entsperren
- Elementdetails anzeigen
- Element löschen
- Eine Datei auf ein lokales oder ein Netzlaufwerk herunterladen
- Ansichtssitzung anhand des erstellten Elements oder der Ordner-URL starten
- Historische Revisionen eines Elements anzeigen
- Die Eigenschaften einer Revision anzeigen
- Den Kommentar einer Revision bearbeiten

Hinweis: Sie müssen über eine StarTeam-Benutzerlizenz verfügen, um den Web-Client verwenden zu können.

Neue Funktionen in anderen StarTeam 2009-Komponenten und -Produkten

Nachfolgend sind die neuen Funktionen bzw. Verbesserungen aufgeführt, die in andere StarTeam-Produkte integriert wurden und in dieser Version enthalten sind.

- Neues in der Dokumentation
- Neue Funktionen in StarTeamMPX
- Neue Funktionen in Layout-Designer

Neues in der Dokumentation

Bei StarTeam 2009 wird in den grundlegenden Anwendungen nun statt des proprietären Hilfe-Browsers von Borland das Ecplise-Infocenter für die Online-Hilfe verwendet. Letztendlich soll das Eclipse-Infocenter in allen Borland-Produkten eingesetzt werden.

Der Eclipse-Browser wird in dieser Version im Cross-Platform-Client, im Serveradministrations-Tool und im Layout-Designer eingeführt. Die kombinierte Hilfedokumentation mit dem Namen "StarTeam verwalten und einsetzen" in Vorgängerversionen wurde ersetzt durch kleinere Dokumentationsteile, die für die jeweils verwendete Anwendung relevant sind. So enthält beispielsweise der Cross-Platform-Client die Client-Hilfe und die Hilfe zu den Befehlszeilen-Tools, einschließlich `VCMUtility`, und das Serveradministrations-Tool enthält nur die Serveradministrations-Hilfe plus der Hilfe für die Befehlszeilen-Tools.

Das Eclipse-Infocenter hat für Sie den Vorteil, dass Sie eine Volltextsuche durchführen und kleine Teile oder ganze Abschnitte aus dem Inhaltsverzeichnis ausdrucken können.

Zudem kann die Hilfe wie üblich auch über das Windows-Startmenü ausgeführt werden. Unter Linux oder Solaris befindet sie sich im Ordner `/PRODUKTNAME/Documentation`.

Hinweis: Die Installationsanweisungen für den Linux-Server wurden in das Installationshandbuch verschoben.

Neue Funktionen in StarTeamMPX

StarTeamMPX 2009 enthält die folgenden neuen Funktionen:

- Die Multicast-Option wurde aus StarteamMPX entfernt.
- Clients abonnieren einen neuen STEvent3-Stream, der differenziertere Subjekte für ansichtsspezifische Ereignisse verwendet. Meldungen werden komprimiert und in Transaktionen zusammengefasst. Für jeden Client verringert sich der Datenverkehr um 70 bis 80 %. Ein StarTeam 2009-Client erhält nur bis zu 2 % der Meldungen und bis zu 2 % des Datenverkehrs verglichen mit einem StarTeam-Client vor Version 2009.
- Bestimmte "doppelte" Cache-Meldungen fallen weg, beispielsweise redundante Meldungen zu Dateiinhalten. Dadurch wird der Datenverkehr zu Cache-Agenten verringert.
- Die Verbesserungen bei Meldungen sind für Clients transparent.
- Wenn Verbindungen von Clients vor StarTeam 2006 nicht zulässig sind, was der Fall ist, wenn das Mindest-API-Level für Server > 1,25 ist, wird der `STEvent`-Event-Stream nicht per Broadcast übertragen. Der `STEvent2`-Event-Stream wird auch dann nicht per Broadcast übertragen, wenn das Mindest-API-Level für Server > 1,66 ist, was bedeutet, dass nur StarTeam 2009 und spätere Clients zulässig sind.
- Neue StarTeam 2009-Ereignisse werden an den `STEvent3`-Stream gesendet, wie z. B. Änderungspakete und Trace-Objekte (externe Links).

Neue Funktionen in Layout-Designer

Der Layout-Designer enthält die folgenden neuen Funktionen in StarTeam 2009

- Die im Cross-Platform-Client bereitgestellten Formulare stehen nun als Beispielformulare im Layout-Designer zur Verfügung.
- Der Layout-Designer verwendet die neue Eclipse-Infocenter-Hilfe. Weitere Informationen hierzu finden Sie unter "Neues in der Dokumentation".

Hilfe zur Hilfe

In diesem Abschnitt wird das Hilfesystem von StarTeam beschrieben. Außerdem wird erklärt, wo sich die Dokumentation der einzelnen StarTeam-Produkte befindet.

In diesem Abschnitt

StarTeam Übersicht

Das StarTeam-Hilfesystem enthält konzeptionelle Themen, Arbeitsanweisungen und Referenzinformationen, die es Ihnen bei Bedarf ermöglichen, von allgemeinen zu spezifischeren Informationen zu navigieren.

Konzeptionelle Themen	Die konzeptionellen Übersichten bieten Informationen zur Produktarchitektur, zu Komponenten und Empfehlungen für die Arbeit mit StarTeam. Am Ende der meisten Themen finden Sie Links zu verwandten Themen, ausführlicheren Informationen und/oder Themen zur Verfahrensweise oder Referenzen.
Themen mit Arbeitsanweisungen	Diese erklären Vorgänge Schritt für Schritt. Für Vorgänge in StarTeam, die mehrere Unteraufgaben enthalten, gibt es Kernverfahren, die die Unteraufgaben enthalten, die für das Ausführen umfassenderer Aufgaben erforderlich sind. Wenn Sie mit der Arbeit an einer Aufgabe beginnen, z. B. mit dem Upgrade eines Servers (im Installationshandbuch) und wissen möchten, welche Schritte erforderlich sind, zeigen Sie das Kernverfahren für den Bereich an, in dem Sie gerade arbeiten. Zusätzlich zu den Kernverfahren gibt es mehrere Verfahren, die einzelne Aufgaben umfassen. Alle Verfahren befinden sich im Bereich "Verfahren" des konsolidierten Hilfesystems. Die meisten konzeptionellen Themen und Referenzthemen bieten zudem Links zu sachdienlichen bzw. verwandten Verfahren.
Referenzinformationen	Die Referenzthemen enthalten ausführliche Informationen zu Themen wie Befehlszeilenoptionen, StarTeam-Feldern und Dateistatusinformationen. Alle Referenzthemen befinden sich im Bereich "Referenz" des konsolidierten Hilfesystems und die meisten der Referenzthemen enthalten Links zu verwandten Verfahren oder konzeptionellen Themen.

Das StarTeam-Hilfesystem besitzt vier Hauptbereiche: Einführung, Konzepte, Verfahren und Referenz. Jeder der Hauptbereiche enthält Unterbereiche, in denen Informationen in funktionale Bereiche zusammengefasst sind. Dies wird in der untenstehenden Tabelle beschrieben.

Dieser Hilfebereich...	Enthält Informationen zu...
Allgemeines	Verfahren und konzeptionelle Informationen für einen Entwickler oder gelegentlichen Benutzer von StarTeam, z. B. zum Ein- und Auschecken von Dateien und zum Festlegen von persönlichen Benutzeroptionen.
Anpassung	Verfahren und konzeptionelle Informationen für einen Benutzer, der StarTeam mit dem Layout Designer anpasst.
Projektadministration	Verfahren und konzeptionelle Informationen für einen StarTeam-Projekt-Administrator, z. B. zum Erstellen von Projekten und Ansichten.
Serveradministration	Verfahren und konzeptionelle Informationen für einen StarTeam-Server-Administrator, z. B. zum Anpassen von Serverkonfigurationen, Sichern von Informationen und Migrieren von Servern.
Sicherheit	Verfahren und konzeptionelle Informationen für einen StarTeam-Server-Administrator, der sich für die in StarTeam verfügbaren Sicherheitsfunktionen interessiert, z. B. für Funktionen zum Verwalten von Benutzern, Gruppen, Zugriffsrechten und Passwörtern.
Konfiguration	Verfahren für die Konfiguration der StarTeam-Clients, z. B. das Hinzufügen einer Serverkonfiguration und das Ändern eines Passworts.
Berichtserstellung und Testen	Auf den StarTeam-Clients verfügbare Verfahren für einen QA-Mitarbeiter oder Projektmanager, z. B. Verfahren zum Erstellen von Diagrammen oder Berichten, zum Arbeiten mit Änderungsanforderungen und zum Abfragen oder Filtern von Daten.

Verwandte Konzepte

StarTeam Produktübersicht
Wo befindet sich die Dokumentation für die einzelnen Produkte

Wo befindet sich die Dokumentation für die einzelnen Produkte

Dieses Thema beschreibt die unterschiedlichen Methoden des Zugriffs auf die StarTeam-Produktdokumentation und enthält eine Liste der mit den einzelnen StarTeam-Produkten ausgelieferten Dokumentation.

So greifen Sie auf die Produktdokumentation zu

In der Regel können Sie auf die Dokumentation für die StarTeam-Produkte wie folgt zugreifen:

- Über das Menü **Hilfe** des jeweiligen Produkts.
- Wenn Sie mit einem Windows-System arbeiten, finden Sie die Dokumentation für die StarTeam-Produkte, indem Sie auf **Start** ▸ **Programme** ▸ **Borland StarTeam** ▸ **<Produkt>** ▸ **Dokumentation** klicken. Im Menü **Dokumentation** ist die gesamte Dokumentation für das ausgewählte Produkt aufgeführt.
- Die Readme-Dateien und Installationsanweisungen befinden sich direkt unter dem Stamminstallationsverzeichnis (oder im Stamm der Installations-CD). Bei Dokumentationen, die in anderen Sprachen (nicht nur in Englisch) verfügbar sind (Japanisch, Französisch oder Deutsch), sind die sprachspezifischen Versionen der Versionshinweise und Installationsanweisungen mit dem entsprechenden _*Ländercode* im Dateinamen gekennzeichnet. Die Datei "readme_ja.html" enthält beispielsweise Informationen in Japanisch. Die PDF-Handbücher finden Sie im Unterordner "Documentation" der Produkt-CDs.
- Die PDF-Handbücher und Online-Hilfe-Dateien finden Sie in den Unterordnern "PDF" bzw. "Hilfe" im Stamminstallationsordner.
- Sie können die Dokumentation auch direkt von der Website "Borland StarTeam Technical Publications" herunterladen: http://info.borland.com/techpubs/starteam .

StarTeam-Produktdokumentation

Bestimmte Teile (jedoch nicht alle) der StarTeam-Dokumentation wurden in dieser Version in ein Hilfesystem konsolidiert. Die einzelnen Produkte und die zugehörige Dokumentation ist im Folgenden aufgeführt.

Dokumentation für StarTeam-Server und StarTeam-Cross-Platform-Client:

Diese Dokumentation ist in Englisch, Japanisch, Französisch und Deutsch verfügbar.

StarTeam Hilfe (Online-Hilfe)	Die Online-Hilfe der StarTeam-Hilfe, die über das Menü **Hilfe** im Fenster "Serveradministration" des Cross-Platform Client und der StarTeam Visual Studio 2005 Integration geöffnet wird.
StarTeam verwalten und einsetzen (AdministeringAndUsingStarTeam.pdf)	Eine identische Version der StarTeam-Hilfe im PDF-Format.
StarTeam Extensions-Benutzerhandbuch (extensions.pdf)	Die PDF-Version der Hilfe für StarTeam Extensions.
StarTeamMPX-Administratorhandbuch (adminMPX.pdf)	Die PDF-Version der Hilfe für StarTeamMPX.
Install_de.pdf	Die sprachspezifische Version des StarTeam-Installationshandbuchs, das viele Produkte in der StarTeam-Produktreihe abdeckt.
readme_de.html	Die sprachspezifische Version der Versionshinweise, die viele Produkte in der StarTeam-Produktreihe abdeckt.

StarTeamWeb Client

Diese Dokumentation ist in Englisch, Japanisch, Französisch und Deutsch verfügbar.

Web Client Hilfe (Online-Hilfe)	Die Eclipse-Browser-Hilfe für die Web Client-Hilfe wird geöffnet innerhalb des Web Client im **Hilfe**menü.

StarTeamMPX

Diese Dokumentation ist in Englisch, Japanisch, Französisch und Deutsch verfügbar.

StarTeamMPX-Administratorhandbuch (adminMPX.pdf)	Die PDF-Version des Administratorhandbuchs für dieses Produkt.
StarTeam installieren (Install_de.pdf)	Die sprachspezifische Version des StarTeam-Installationshandbuchs, das viele Produkte in der StarTeam-Produktreihe abdeckt.
Versionshinweise (readme_de.html)	Die sprachspezifische Version der Versionshinweise, die viele Produkte in der StarTeam-Produktreihe abdeckt.

StarTeam Workflow Extensions

Diese Dokumentation ist in Englisch, Japanisch, Französisch und Deutsch verfügbar.

StarTeam Extensions-Benutzerhandbuch (extensions.pdf)	Die PDF-Version des Benutzerhandbuchs für dieses Produkt.
StarTeam installieren (Install_de.pdf)	Die sprachspezifische Version des StarTeam-Installationshandbuchs, das viele Produkte in der StarTeam-Produktreihe abdeckt.
Versionshinweise (readme_de.html)	Die sprachspezifische Version der Versionshinweise, die viele Produkte in der StarTeam-Produktreihe abdeckt.

Borland LDAP QuickStart Manager

Diese Dokumentation ist in Englisch, Japanisch, Französisch und Deutsch verfügbar.

LDAP QuickStart Manager Guide (LDAPQuickStart.pdf)	Die PDF-Version des Benutzerhandbuchs für dieses Produkt.
Versionshinweise (readme_LDAP_de.html)	Versionshinweise für LDAP QuickStart Manager.
Installationsanweisungen (install_LDAP_de.html)	Installationsanweisungen für LDAP QuickStart Manager.

Borland Search

Diese Dokumentation ist in Englisch, Japanisch, Französisch und Deutsch verfügbar.

Borland Search-Administratorhandbuch (SearchInstallAdmin.pdf)	Die PDF-Version des Benutzerhandbuchs für dieses Produkt.
Versionshinweise (readme_BorlSearch.html)	Versionshinweise für Borland Search.
Installationsanweisungen (install_BorlSearch.html)	Installationsanweisungen für Borland Search.

StarTeam SDK

SDK-Entwicklerhandbuch	HTML-Version des Entwicklerhandbuchs für das StarTeam-SDK.
Java-API-Referenz	Java-Dokumentation für das StarTeam-SDK.
COM-API-Referenz	COM-Build-Blöcke für das StarTeam-SDK.
Versionshinweise (readme_SDK.html)	Versionshinweise für das StarTeam-SDK.

StarTeam Datamart

StarTeam Datamart-Benutzerhandbuch (StarTeam Datamart User Guide.pdf)	Die PDF-Version des Benutzerhandbuchs für dieses Produkt.
Versionshinweise (readme_Datamart_de.html)	Versionshinweise für StarTeam Datamart.

Der Import/Export-Manager in StarTeam

StarTeam Import/Export Manager-Benutzerhandbuch (stiemgr.pdf)	Die PDF-Version des Benutzerhandbuchs für dieses Produkt.
Versionshinweise (readme_IEM.html)	Versionshinweise für StarTeam StarTeam Import/ Export Manager.
Installationsanweisungen (install_IEM.html)	Installationsanweisungen für StarTeam StarTeam Import/Export Manager.

StarTeam Toolbar-Dienstprogramm

Die StarTeam-Toolbar verwenden (SBToolbar.pdf)	Dies PDF-Version des Benutzerhandbuchs für dieses Produkt finden Sie, wenn Sie auf den Schalter **Hilfe** in StarTeam Toolbar-Dienstprogramm klicken.

Verwandte Konzepte

StarTeam Produktübersicht
StarTeam Übersicht
Einführung in die Benutzeroberfläche

Benutzerrollen und StarTeam-Dokumentation

Dieses Thema enthält Informationen zu unterschiedlichen Benutzerrollen und die damit verbundene Dokumentation. Diese Rollenfunktionen entsprechen möglicherweise den in Ihrer Organisation verwendeten Rollen, dienen hier aber als Beispiel für Situationen, in denen Vorgänge auf mehrere StarTeam-Benutzer aufgeteilt werden.

Die empfohlenen Rollen für StarTeam sind im Folgenden zusammen mit Informationen darüber angegeben, wo Sie die entsprechenden Verfahren und konzeptionellen Themen zu diesen Rollen finden.

Benutzer/Entwickler	Ein Benutzer ist primär damit beschäftigt, Dateien ein- oder auszuchecken, zusammenzuführen und Änderungsanforderungen zu schließen. Weitere Informationen zu den mit dieser Benutzerrolle verknüpften Konzepten und Abläufen finden Sie unter den Knoten "Allgemeines" in der konsolidierten Dokumentation.
Projektmanager/Super User	Diese Rolle umfasst verfahrensspezifische sowie konzeptionelle Informationen aus den Abschnitten "Allgemeines", "Projektadministration" und "Serveradministration".
Tester	Diese Rolle ist beispielsweise für einen Benutzer in einem QA-Team vorgesehen. Weitere Informationen zu Benutzern in dieser Rolle finden Sie in den Abschnitten "Allgemeines" und "Tester" der Dokumentation.
Administrator	Diese Rolle umfasst die Installation, Konfiguration und Verwaltung von StarTeam. Die Themen aus den Abschnitten "Serveradministration" und "StarTeam installieren und konfigutieren" der Dokumentation enthalten konzeptionelle und verfahrensspezifische Informationen zu dieser Benutzerrolle.
Customizer	Ein Benutzer, der Anpassungen an StarTeam unter Verwendung alternativer Eigenschaftseditoren und Funktionen vornimmt, die mit StarTeam Extensions und dem StarTeam Layout-Designer installiert werden. Informationen zum StarTeam Layout-Designer und zum Erstellen von benutzerdefinierten Eigenschaftsfeldern finden Sie in der Dokumentation in den Abschnitten zur Anpassung. Weitere Informationen zur Verwendung alternativer Eigenschaftseditoren und zum Ändern des in StarTeam integrierten Workflows finden Sie im StarTeam Extensions-Benutzerhandbuch (extensions.pdf).

Richtlinien für die Bereitstellung von StarTeam

In diesem Abschnitt werden die Hardware-Bereitstellungsoptionen für StarTeam erläutert. Da StarTeam sowohl von kleinen Teams als auch von kleinen, mittleren und großen Unternehmen eingesetzt werden kann, gibt es eine Vielzahl von Bereitstellungsoptionen für die Komponenten, die sich auf Performance, Skalierbarkeit, Failover und andere Faktoren auswirken, wie z. B. minimale Hardware-Anforderungen, Optionen für Hochverfügbarkeit sowie Optionen für verteilt arbeitende Teams.

In diesem Abschnitt

Leistungs- und Skalierbarkeitsfaktoren

StarTeam ist eine umfangreiche Anwendung, die auf vielfältige Weise eingesetzt werden kann. Aufgrund dieser Flexibilität kann jedoch nicht von vornherein eindeutig geklärt werden, wie eine optimale Hardwarekonfiguration in Ihrer Organisation auszusehen hat. Dies sind die wichtigsten Faktoren, die sich auf die Leistungsfähigkeit und Skalierbarkeit einer StarTeam-Konfiguration auswirken:

- **Größe des Repository:** Die Anzahl der Ansichten und Elemente hat größere Auswirkungen auf die Speichernutzung der StarTeam-Serverprozesses, die Anzahl der Datenbankabfragen und andere Ressourcenfaktoren als andere Datentypen. Diese Typen (z. B. Benutzer, Gruppen, Abfragen und Filter) wirken sich in geringerem Maß auf die Ressourcennutzung aus. Kurz gesagt, bei einem zunehmenden Repository wachsen die Anforderungen an das Server-Caching und die Datenbankabfragen.
- **Gleichzeitige Benutzer:** Die Anzahl der *gleichzeitigen* Benutzer zu Spitzenzeiten hat signifikante Auswirkungen auf einen Server. Für jeden dieser Benutzer ist eine *Sitzung* erforderlich, die einen Status hat, Befehle generiert (die Worker-Threads verwenden), Sperren einrichtet usw. Die Anzahl der *definierten* Benutzer ist nicht annähernd so bedeutend wie die Anzahl der gleichzeitigen Benutzer zu Spitzenzeiten. Bei der Kapazitätsplanung sollten Sie die Anzahl der gleichzeitigen Benutzer als Faktor heranziehen.
- **StarTeamMPX:** MPX erhöht die Server-Skalierbarkeit. Diese ist daher davon abhängig, ob Sie MPX zum Einsatz bereitstellen und auf den Clients aktivieren oder nicht. MPX-Cache-Agenten erhöhen nicht nur für Remote-Benutzer die Performance beim Auschecken, sondern reduzieren auch erheblich den Netzwerkverkehr des Servers. Kurz gesagt, die Bereitstellung von MPX erhöht die Skalierbarkeit der Konfiguration.
- **Bulk-Anwendungen:** Online-Benutzer, die einen grafischen Client verwenden, belasten den Server in der Regel nur geringfügig. Bulk-Anwendungen hingegen, z. B. "Extraktoren" für StarTeam Datamart oder Borland Search, und "Synchronisierer" für Integrationen, wie z. B. Borland CaliberRM oder Mercury Quality Center, senden in der Regel über längere Zeiträume fortlaufende Befehlsströme. Eine einzige Bulk-Anwendung kann den Server so sehr belasten wie 10 bis 20 Online-Benutzer.
- **Anwendungskomplexität:** Aufgrund der Anpassbarkeit von StarTeam ist es möglich, umfangreiche, benutzerdefinierte Formulare zu erstellen, zahlreiche benutzerdefinierte Felder zu Artefakttypen hinzuzufügen, benutzerdefinierte Berichte zu generieren usw. Je umfangreicher Sie das System nutzen, desto mehr Befehle werden generiert und desto größer werden die Artefakte. Beides erhöht die Anforderungen an den Server.

Diese Faktoren sollten Sie beachten, wenn Sie die Größe Ihrer Konfiguration festlegen. Da die einzelnen Umgebungen über einzigartige Merkmale verfügen, handelt es sich bei diesen Vorschlägen nur um Richtlinien.

Größe der Konfiguration

Es gibt keine festen Regeln, anhand derer die Größe einer StarTeam-Konfiguration (*klein*, *mittel* oder *groß*) definiert werden kann. In diesem Dokument wird als definierender Faktor die Anzahl der gleichzeitigen Benutzer herangezogen:

- Eine *kleine Konfiguration* unterstützt maximal 50 gleichzeitige Benutzer.
- Eine *mittlere Konfiguration* unterstützt maximal 100 gleichzeitige Benutzer.
- Eine *große Konfiguration* unterstützt mehr als 100 gleichzeitige Benutzer.

Für die Bereitstellungsplanung scheint die Anzahl der gleichzeitigen Benutzer - also nicht das Datenvolumen oder die Benutzertypen - der beste Anhaltspunkt dafür zu sein, welche Konfigurationsgröße zu wählen ist. Erfahrungsgemäß nimmt die Datenmenge, die von einer StarTeam-Konfiguration verwaltet wird (insbesondere Elemente), proportional zur Anzahl der Projekte und Ansichten zu, die wiederum im Verhältnis zur Teamgröße zunimmt. Darüber hinaus bleibt bei unterschiedlich großen Organisationen das Verhältnis zwischen Online-Benutzern und Bulk-Anwendungen ungefähr gleich.

Wie groß kann eine Konfiguration maximal angelegt werden? Derzeit gibt es vereinzelte StarTeam-Instanzen mit mehr als 500 gleichzeitigen Benutzern, mehr als 10.000 "definierten" Benutzern, über 4.000 Ansichten, Elementen im achtstelligen Bereich oder bis zu einem Terabyte Daten im Datenspeicher. Fortschritte bei Hard- und Software führen dazu, dass diese Grenzwerte jedes Jahr übertroffen werden.

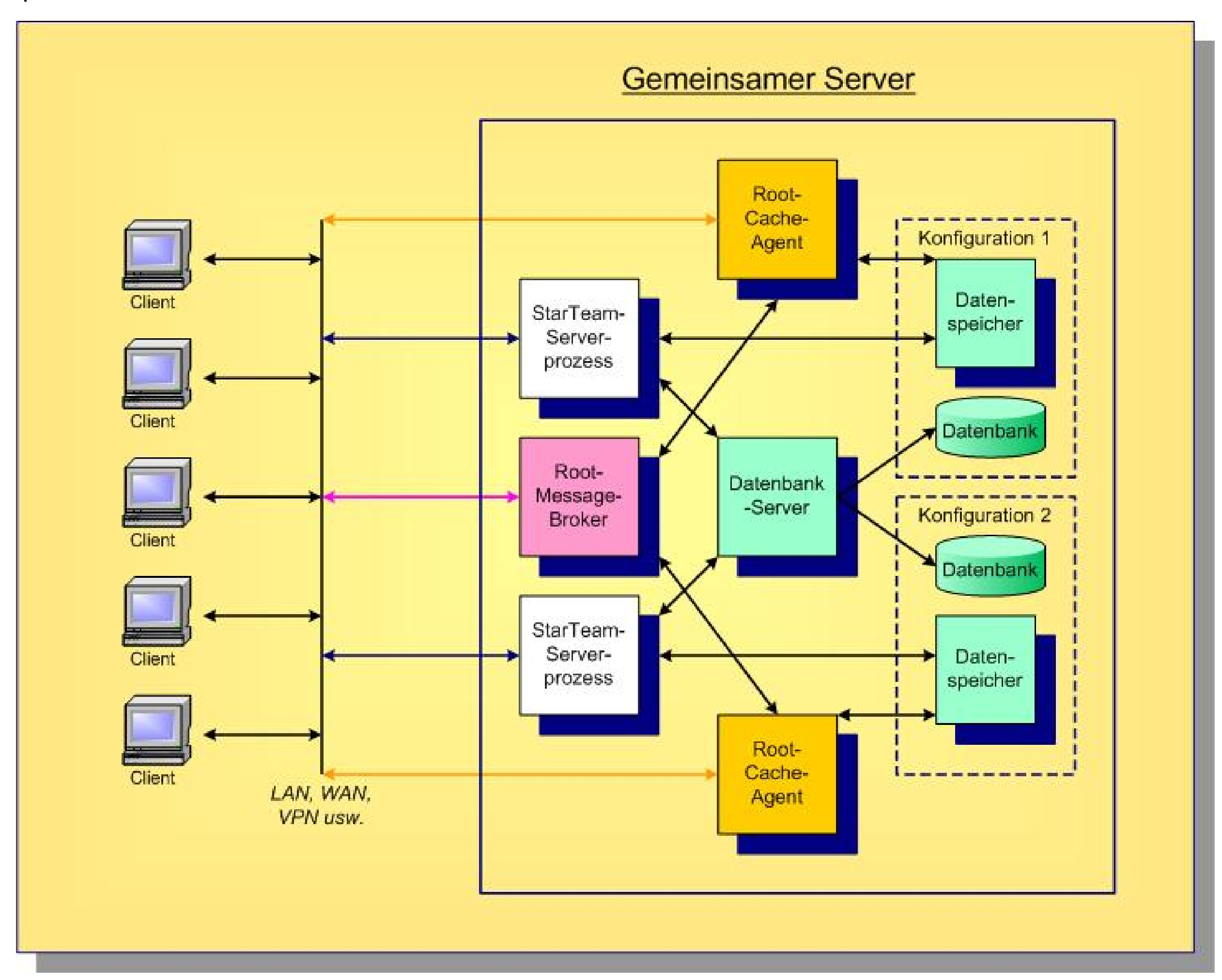
Hinweis: Diese Werte wurden nicht alle in derselben Konfiguration erzielt. Einige Kunden verfügen zwar über 4.000 Ansichten, diese werden aber nicht alle aktiv genutzt. Bei einem Kunden mit 10.000 Benutzern sind zu Spitzenzeiten in der Regel 250-300 Benutzer gleichzeitig aktiv. Interessanterweise scheint sich die Datenmenge im Speicher nur geringfügig auf die Leistung oder Skalierbarkeit auszuwirken.

Die folgenden Faktoren sind bei großen Konfigurationen zu beachten:

- **Startzeit:** Der StarTeam-Serverprozess führt beim Start bestimmte Wartungsaufgaben durch, z. B. Bereinigung veralteter Audit- und Sicherheitsdaten in der Datenbank. Wenn sich die Anzahl der Aktivitäten erhöht und der Abstand zwischen Neustarts zunimmt, verlängern diese Aufgaben die Programmstartzeit. Die Startzeit wird außerdem von der Anzahl der eindeutigen "Freigabebäume" beeinflusst, da beim Startvorgang Cache-Speicher erstellt werden. Bei einer optimalen Konfiguration können sogar große Server innerhalb von wenigen Minuten gestartet werden. Der Vorgang kann jedoch auch bis zu 15 Minuten oder länger in Anspruch nehmen.
- **Speichernutzung:** Die Speichernutzung des StarTeam-Serverprozesses wird durch verschiedene Faktoren beeinflusst, z. B. die Gesamtanzahl der Elemente, die Einstellungen der Server-*Caching*-Option, die Anzahl der aktiven Sitzungen (gleichzeitige Benutzer), der aktiven Ansichten sowie der erforderlichen Befehls-Threads. Die Caching-Optionen können im eingeschränkten Umfang zum Steuern der Speichernutzung verwendet werden. Sitzungen, aktive Ansichten und andere Faktoren, die sich auf die Laufzeit auswirken, erfordern jedoch einen gewissen Umfang an Arbeitsspeicher. Auf einer 32-Bit-Windows-Plattform ist der StarTeam-Serverprozess auf einen virtuellen Speicher von 2 GB begrenzt. Wenn Sie die 4GT RAM Tuning-Funktion aktivieren, wird der virtuelle Speicher auf einem 32-Bit-System für einen einzelnen Prozess auf einen Wert von fast 3 GB erweitert.
- **Befehlsgröße:** Einige Client-Anforderungen geben unterschiedlich große Antworten zurück. Dies ist von der Anzahl der angeforderten Elemente, der definierten Benutzer oder Gruppen, der Labels einer Ansicht usw. abhängig. Große Serverkonfigurationen führen bei bestimmten Befehlen dazu, dass umfangreiche Antworten zurückgegeben werden, die für hohe Übertragungszeiten verantwortlich sind, insbesondere in langsamen Netzwerken. Bei Clients wirkt sich dies in Form von schlechterer Performance bei bestimmten Operationen aus, z. B. beim Öffnen eines Projekts oder eines benutzerdefinierten Formulars.

Mehrere Konfigurationen auf demselben Server

Bei kleineren bis mittlerenServerkonfigurationen können Sie alle StarTeam-Server-Komponenten auf einem einzelnen Rechner platzieren. Außerdem können Sie alle Komponenten für mehrere Konfigurationen auf demselben Rechner zum Einsatz bereitstellen. Dies hängt von der **Anzahl** der Benutzer ab, die gleichzeitig auf **alle** Konfigurationen zugreifen. Die Abbildung unten zeigt für den Einsatz bereitgestellte Basis- und MPX StarTeam-Komponenten.



Sie sollten für alle StarTeam-Serverkomponenten nur dann einen einzelnen Rechner verwenden, wenn bei allen Konfigurationen zusammengenommen 100 oder weniger gleichzeitige Benutzer zu erwarten sind. Eine einzelne Konfiguration unterstützt zwar mehr als 100 Benutzer, aber jede Konfiguration verfügt über einen gewissen Umfang an Overhead. Daher wird empfohlen, mindestens eine Konfiguration auf einem separaten Rechner auszuführen, wenn zu Spitzenzeiten 100 gleichzeitige Benutzer aktiv sind.

Wenn ein einzelner Rechner eingesetzt wird, werden alle StarTeam-Serverprozesse, der Root-Message-Broker, die Root-Cache-Agenten und der Datenbankserverprozess auf einem Rechner ausgeführt. Für dieses Layout gelten folgende Faustregeln:

- Beginnen Sie mit einer CPU und 1 GB Arbeitsspeicher für den Datenbankserverprozess.
- Fügen Sie **pro** StarTeam-Konfiguration eine CPU und 1 GB Arbeitsspeicher hinzu.
- Wenn Sie für den Datenspeicher und die Datenbankpartitionen der einzelnen StarTeam-Konfigurationen jeweils eine lokal angeschlossene Festplatte verwenden, sollten Sie separate und schnelle Laufwerk einsetzen, um die Leistungsfähigkeit bei gleichzeitiger Nutzung zu optimieren. Außerdem sollten die Festplatten gespiegelt werden, um ein "Single Point of Failure" zu vermeiden.

- Wenn Sie MPX zum Einsatz bereitstellen, nutzen alle StarTeam-Konfigurationen gemeinsam einen Root-MPX-Message-Broker. Aus der Abbildung wird nicht ersichtlich, dass ein oder mehrere Remote-Message-Broker an den Root-Message-Broker angebunden werden können.
- Beachten Sie beim Bereitstellen von Cache-Agenten, dass für die einzelnen Konfigurationen Root-Cache-Agenten erforderlich sind, die den Root-Message-Broker gemeinsam nutzen können. Aus der Abbildung wird nicht ersichtlich, dass ein oder mehrere Remote-Cache-Agenten an jeden Root-Cache-Agenten angebunden werden können.
- Achten Sie darauf, die StarTeam-Server, Message Broker, und Root-Cache-Agenten zu konfigurieren, sodass sie TCP/IP-Verbindungen an unterschiedlichen Ports empfangen.

Anhand dieser Richtlinien können drei bis vier kleine StarTeam-Konfigurationen auf einem Rechner bereitgestellt werden - jedoch nur, *wenn* die Gesamtanzahl der gleichzeitigen Benutzer zu Spitzenzeiten den Wert 100 nicht überschreitet. Anderenfalls kommt es aufgrund von fehlenden Ressourcen (CPU, Arbeitsspeicher, Festplatten-I/O und/oder Netzwerkbandbreite) ggf. zu Konflikten zwischen den Prozessen, was sich negativ auf die Leistungsfähigkeit auswirkt. Wenn Sie zunächst eine Konfiguration mit einem Server einrichten, sollten Sie einplanen, die Komponenten bei zunehmender Nutzung auf separate Rechner zu verteilen.

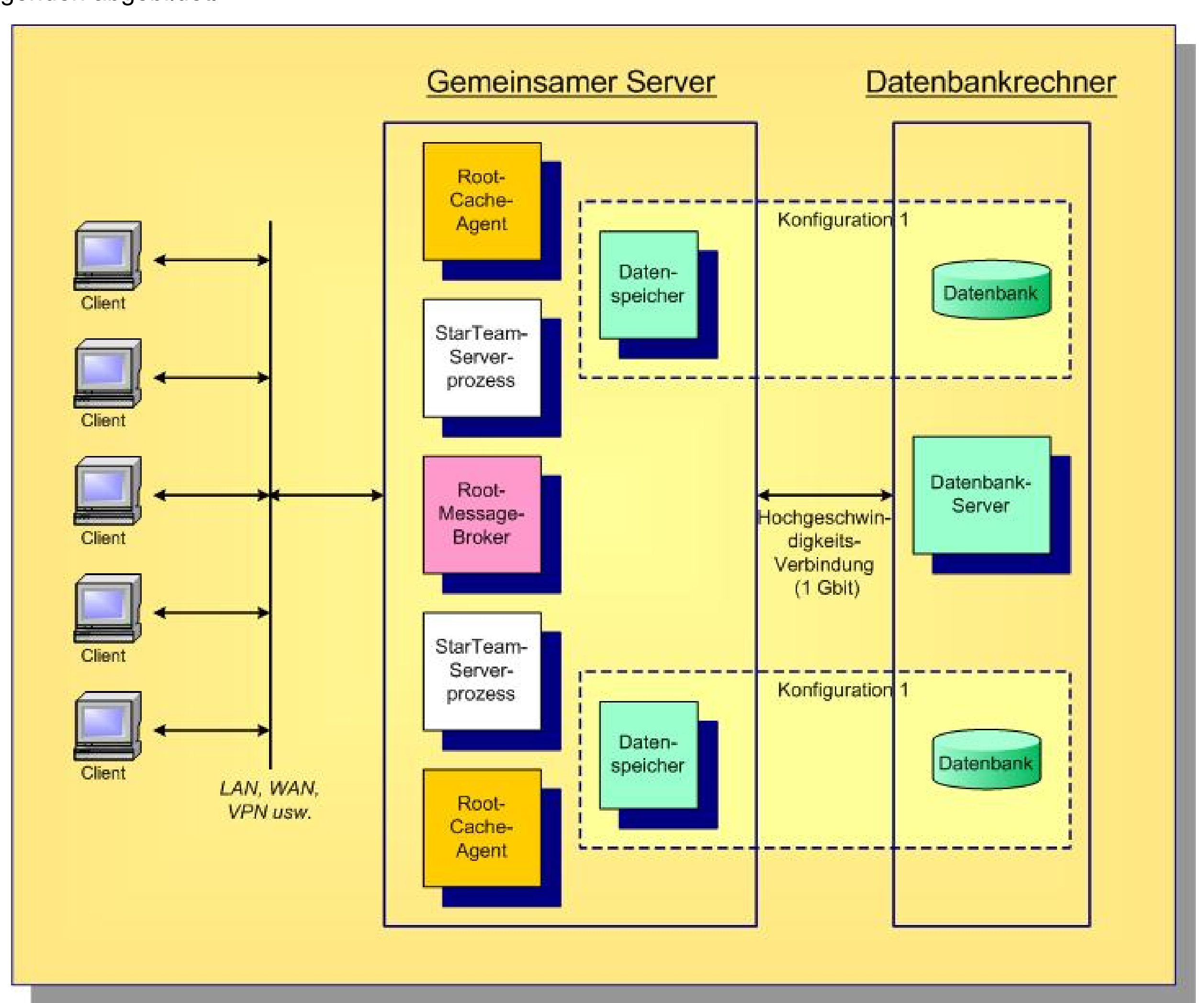
Warnung: Die Bereitstellung mehrerer Konfigurationen auf einem einzelnen Rechner hat den Nachteil, dass sie alle von einem Upgrade des Rechners, einer Patch-Installation oder einer Unterbrechung der Stromzufuhr zum Rechner usw. betroffen sind.

Mittlere Konfigurationen

Wenn Ihre Konfiguration von einer kleinen zu einer mittleren Konfiguration anwächst, sollte als erstes der Datenbankprozess auf einen separaten Rechner ausgelagert werden. Dort sollte eine dedizierte Hochgeschwindigkeitsverbindung (1 GBit) zum StarTeam-Server installiert werden. Die Erfahrung zeigt, dass dadurch die Trennung von Datenbank und Datenbankrechner nahtlos überbrückt werden kann.

Separater Datenbankrechner

Auch wenn für den Datenbankserver ein eigener Rechner verwendet wird, können weiterhin mehrere StarTeam-Serverprozesse und MPX-Komponenten auf demselben gemeinsam genutzten Server zum Einsatz bereitgestellt werden. Da die Verarbeitung der Datenbank an einen anderen Rechner weitergegeben wird, kann die Gesamtanzahl der aktuellen Benutzer höher sein (bis zu ca. 200-300 Benutzer). Ein gemeinsam genutzter Datenbankserver ist im Folgenden abgebildet.

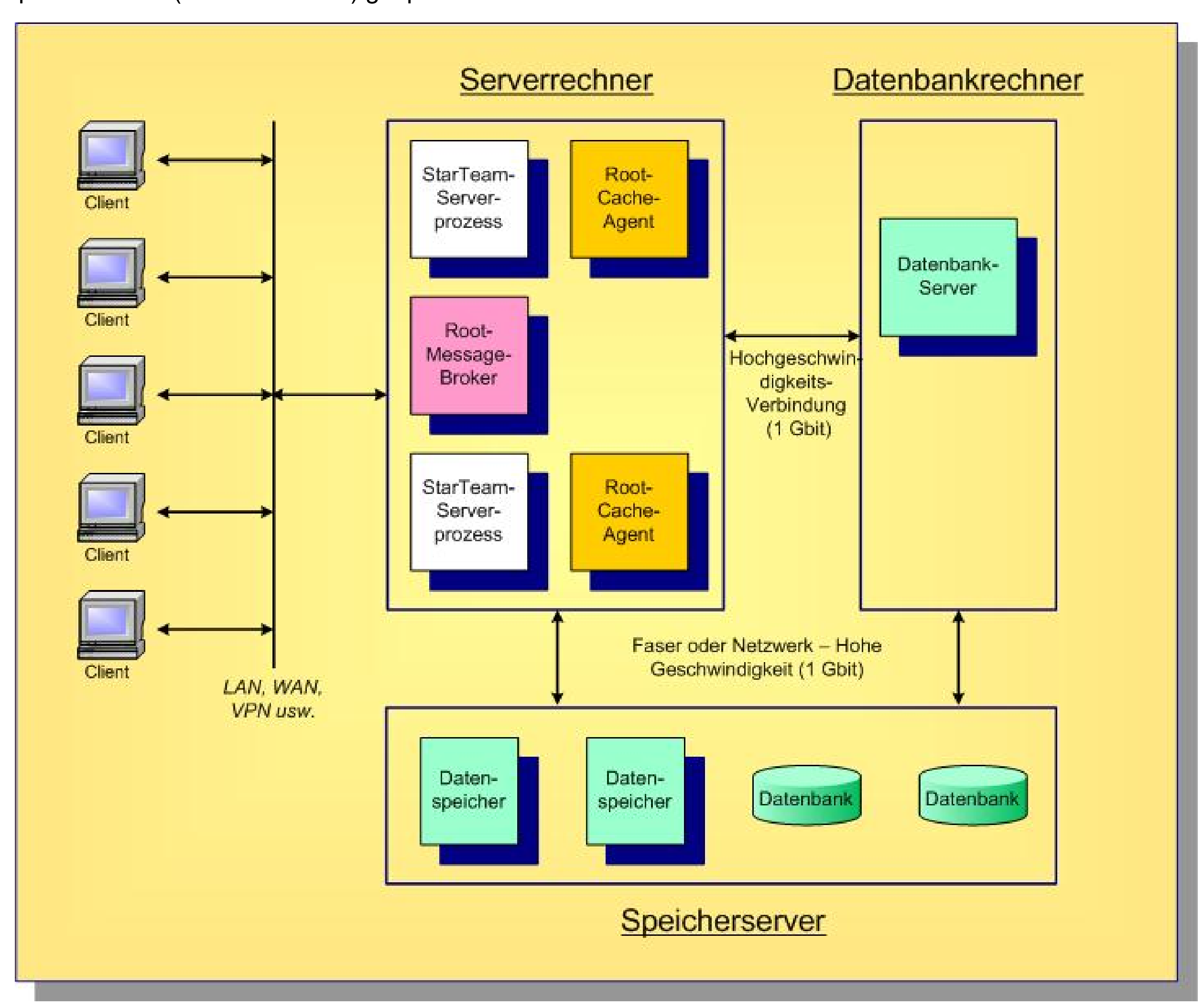


In dieser Abbildung wird angenommen, dass der Server- und Datenbankrechner über eine lokal angeschlossene Festplatte verfügen.

Speicherserver

Bei mehreren Konfigurationen gibt es mehrere Datenspeicher und Datenbanken, ggf. auf verschiedenen Festplatten. Backup-Verfahren und das Spiegeln von Datenbanken für eine hohe Verfügbarkeit sowie andere administrative

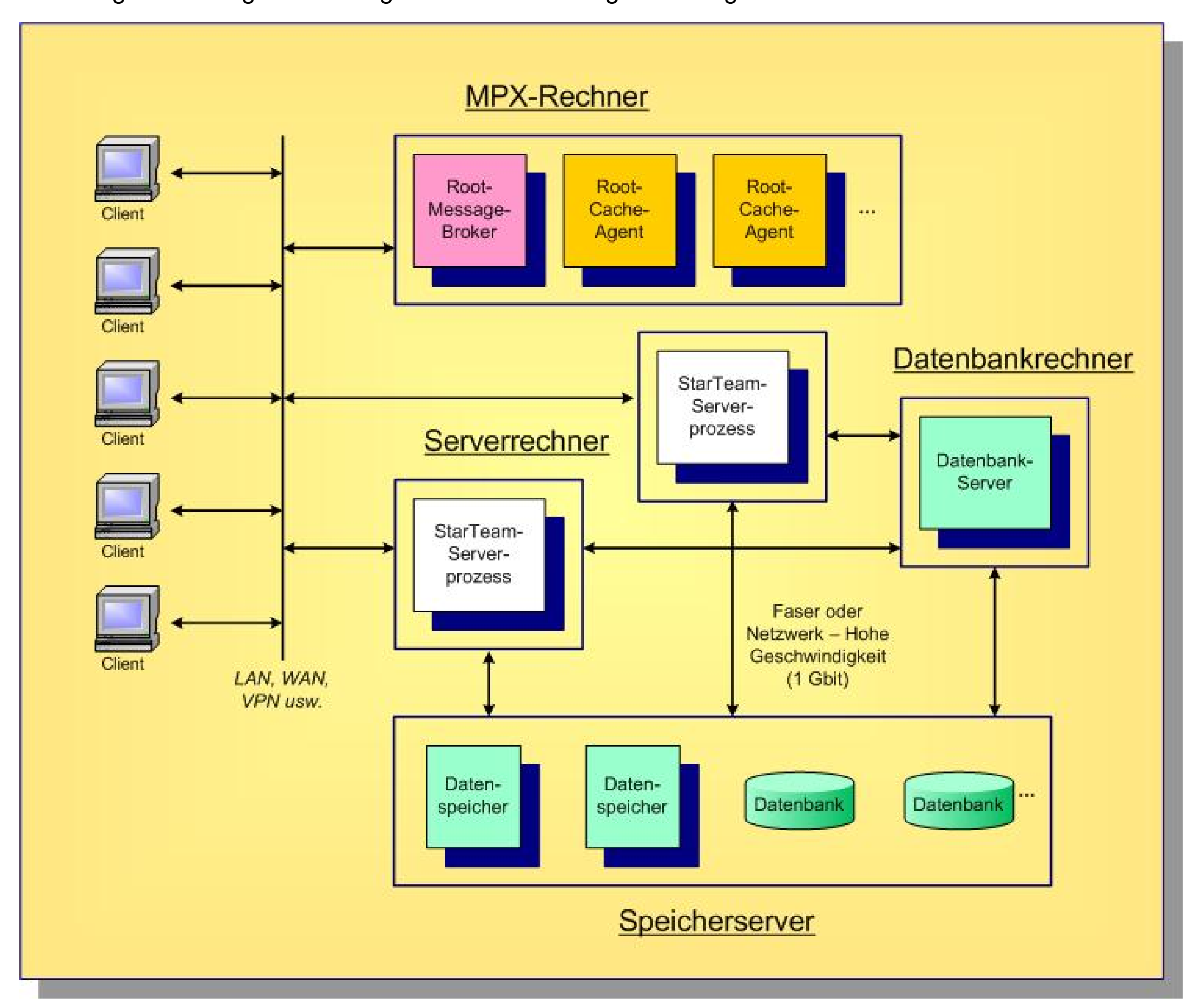
Aufgaben sind ggf. kostengünstiger durchzuführen, wenn alle beständigen Daten auf einem gemeinsam genutzten Festplattenserver (SAN oder NFS) gespeichert sind.



Es ist von Vorteil, einen gemeinsam genutzten Speicherserver für alle Datenspeicher und Datenbanken der Konfigurationen zu verwenden. Je nach Speicherungssystem können alle wichtigen Daten mit einem einzelnen Verfahren gesichert werden. Die für das Spiegeln erforderliche Hardware bzw. andere RAID-Konfigurationen können an einem Standort konzentriert werden. Bei vielen Speicherungssystemen können zusätzliche Festplatten dynamisch hinzugefügt oder eine fehlerhafte Disk im laufenden Betrieb ausgetauscht werden (Hot Swapping).

Große Konfigurationen

Eine große Konfiguration unterstützt 100 gleichzeitige Benutzer bzw. zu Spitzenzeiten auch mehr als 100 Benutzer. Bei einer solchen Konfiguration sollte der StarTeam-Serverprozess auf einem separaten System eingerichtet werden. Auch der Datenbankprozess sollte auf einem eigenen Rechner ausgeführt werden. Es kann von Vorteil sein, den Root-MPX-Message-Broker und die Cache-Agent-Prozesse auf einem eigenen "MPX"-Rechner auszuführen, dies ist jedoch nicht unbedingt erforderlich. Besonders, wenn mehr als 200 bzw. bis zu 300 gleichzeitige Benutzer zu erwarten sind, werden durch die Auslagerung von MPX-Prozessen auf einen separaten Computer starker Netzwerkverkehr und Ressourcenknappheit auf dem StarTeam-Server vermieden. Die typische Bereitstellung mehrerer großer Konfigurationen ist im Folgenden abgebildet.



Die Schlüsselpunkte der Bereitstellung mehrerer großer Konfigurationen sind folgende:

- Die StarTeam-Serverprozesse der einzelnen Konfigurationen werden auf separaten Rechnern ausgeführt. Dies ist in der Regel ein High-End-Rechner mit einer Multi-Core-CPU und mindestens 4 GB Arbeitsspeicher. Wenn es mehr als 100 gleichzeitige Benutzer gibt, empfiehlt Borland die Verwendung eines Rechners mit mindestens einer Quad-Core-CPU und 4 GB Arbeitsspeicher. Wenn zu erwarten ist, dass die Gesamtanzahl der Benutzer weiter zunimmt, wird empfohlen, mit dem leistungsfähigeren Rechner zu beginnen.
- Der Datenbankserver wird auf einem separaten Rechner ausgeführt. Auf diesen Server können mehrere StarTeam-Konfigurationen zugreifen. (Es gibt Erfahrungen mit bis zu acht Konfigurationen, die denselben Datenbankserver ohne Performance-Einbußen verwenden.) Die einzelnen StarTeam-Konfigurationen

verwenden eigene "Schemainstanzen". Jeder StarTeam-Server sollte über eine dedizierte Hochgeschwindigkeitsverbindung (1 GBit) zum Datenbankrechner verfügen.

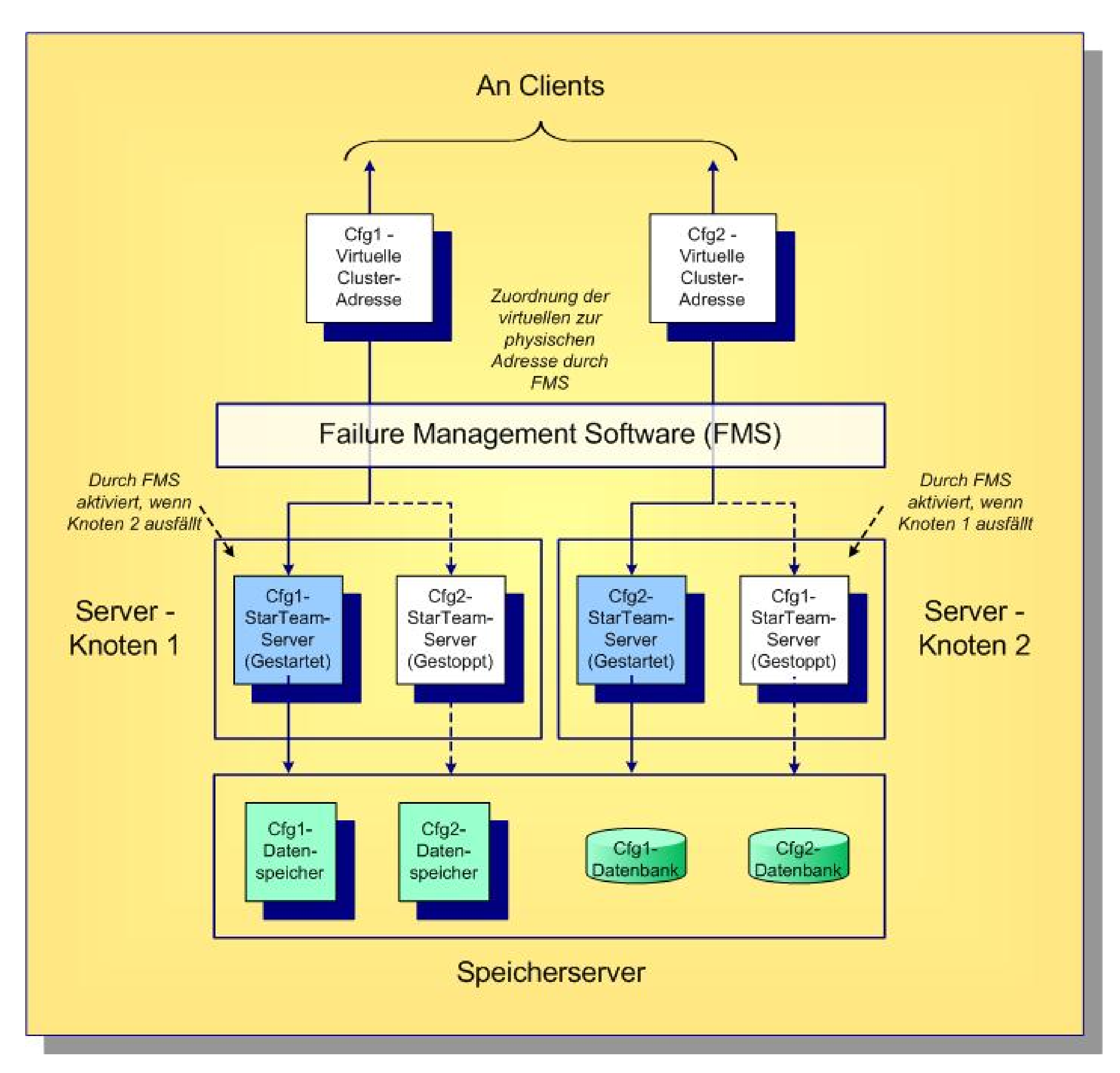
- Der Root-MPX-Message-Broker und die Root-Cache-Agenten können auf einem "MPX-Rechner" ausgeführt werden. Die Root-Cache-Agenten benötigen Zugriff auf die entsprechenden Datenspeicher, eine dedizierte Hochgeschwindigkeitsverbindung ist jedoch nicht erforderlich. Der Dateizugriff über das Netzwerk (z. B. über UNC-Pfade) reicht aus. Wenn Sie einen Notification Agent für den Workflow einsetzen möchten, können Sie diesen ebenfalls auf dem MPX-Rechner betreiben.
- Alle StarTeam-Datenspeicher und -Datenbankpartitionen können einen Speicherserver (z. B. einen SAN-Server) gemeinsam nutzen. Für den Zugriff auf den SAN-Server ist ggf. - abhängig von der Hardware - eine Schnittstelle (z. B. eine "Host"-Karte) für die einzelnen StarTeam-Serverrechner erforderlich.

Aktives/Passives Clustering

StarTeam unterstützt *aktives/passives Clustering*, bei dem ein Standby-Knoten für ein schnelles Failover bereitgehalten wird. Beachten Sie, dass für eine Konfiguration immer nur ein StarTeam-Serverprozess aktiv sein kann. StarTeam-Konfigurationsdateien können jedoch kopiert und zusammen mit der erforderlichen Software auf mehreren Rechnern eingesetzt werden. Außerdem können mehrere Rechner mit Failure Management Software (FMS) eine Verbindung zu derselben Datenbank (bei der es sich ggf. auch um einen Cluster handelt) und zu demselben gemeinsam genutzten Speicherserver für den Datenspeicherzugriff herstellen.

So funktioniert aktives/passives Clustering: Auf einem Knoten im Cluster wird ein StarTeam-Serverprozess gestartet. Dieser wird zum aktiven Knoten in der Konfiguration. Die IP-Adresse des aktiven Knotens wird einer virtuellen "Cluster-Adresse" zugeordnet, zu der Clients eine Verbindung aufbauen. Wenn der aktive Knoten ausfällt, übernimmt die FMS das Failover: Der StarTeam-Serverprozess wird auf einem passiven Rechner gestartet, dieser wird zum aktiven Knoten und ordnet die Cluster-Adresse der IP-Adresse des neuen aktiven Knotens zu. Clients, die ausgeführt werden, erhalten eine Meldung über die Verbindungstrennung und müssen sich neu verbinden. In den meisten Fällen wird das Failover sehr schnell durchgeführt, sodass Clients die Verbindung sofort wiederherstellen können.

Wenn Sie über mehrere StarTeam-Konfigurationen verfügen, können Sie Rechner "paarweise" anordnen, sodass der aktive Knoten einer Konfiguration der passive Knoten einer anderen Konfiguration ist und umgekehrt. So werden beide Rechner aktiv verwendet und nur bei einem Failover muss ein Rechner die Verarbeitung für beide Konfigurationen übernehmen. Ein Beispiel für eine aktive/passive Cluster-Konfiguration finden Sie in der folgenden Abbildung.



In diesem Beispiel sind die StarTeam-Konfigurationen Cfg1 und Cfg2 "gepaart". Daher ist für jede Konfiguration ein Knoten aktiv und ein Knoten passiv. (Der Datenbankprozess ist nicht abgebildet, dieser kann ebenfalls auf einem Cluster zum Einsatz bereitgestellt werden.)

Serveradministration

Die Themen in diesem Abschnitt enthalten einführende Informationen zu StarTeam-Funktionen und Konzepten, die von einem Serveradministrator verwendet werden.

In diesem Abschnitt

Übersicht über die Serveradministration

Der Server verwaltet Daten für alle seine Client-Anwendungen. Der Server wird von einem Serveradministrator verwaltet, der mit den Komplexitäten und Details des Serverbetriebs vertraut ist. Client-Anwendungen, z. B. der Cross-Platform Client, stellen eine Verbindung zum Server her, um auf Daten zugreifen zu können. Als Serveradministrator, der den Server erstmalig installiert, können Sie einige oder alle der folgenden Aktionen ausführen:

- Den Server installieren
- Den Server konfigurieren
- Den Server registrieren (Lizenz)
- Eine neue Serverkonfiguration (eine Instanz des Servers) erstellen und starten
- StarTeamMPX für die neue Serverkonfiguration einrichten
- Neue Benutzer und Gruppen zur Serverkonfiguration hinzufügen
- Den Verzeichnisserver einrichten und Borland LDAP QuickStart Manager zum Hinzufügen von Benutzern verwenden
- Passwortrichtlinien für Nicht-LDAP-Benutzer einrichten
- Projekte und Ansichten für die Serverkonfiguration erstellen
- Zugriffsrechte für Projekte einrichten
- Diagnosefunktionen für die Serverkonfiguration einrichten
- E-Mail-Benachrichtigungen einrichten und die automatische E-Mail-Benachrichtigung mit Ihren eigenen text- oder HTML-basierten Vorlagen für E-Mail-Nachrichten anpassen
- Systemrichtlinien einrichten, d. h. Passwörter, Fehlschläge bei der Anmeldung, Zugriffsrechte und Sicherheitsereignisse für die Serverkonfiguration verwalten

Ab StarTeam Server 2009 erstellt der Server neue Projekte, bei denen nur der Typ "Datei" als Vorgabe für neue Ansichten vorab ausgewählt ist. Benutzer können die Projekteigenschaften nach wie vor nach Erstellen des Projekts ändern und sie können auch die aufgenommenen Elementtypen für eine neue Ansicht ändern. Wenn allerdings der Benutzer nichts ändert, enthalten neue Ansichten nur dann standardmäßig Dateien, wenn sie erstellt werden.

Hinweis: Diese Änderung wirkt sich nicht auf vorhandene Projekte aus. Sie betrifft nur neue Projekte, die mit StarTeam Server 2009 oder vorhandenen Servern, die auf StarTeam Server 2009 aktualisiert wurden, erstellt wurden. Durch das Hinzufügen von anderen Elementtypen zu den Projekteigenschaften (nachdem die Ansicht erstellt wurde) wird die Ansicht NICHT mit den Elementen gefüllt, die in der übergeordneten Ansicht enthalten waren (aber während des Erstellens der neuen Ansicht übergangen wurden). Falls der Benutzer die vorherigen Elemente in die neue Ansicht aufnehmen möchte, muss er sie abrufen, indem er die Basis von der übergeordneten Ansicht ändert.

Ein Server kann eine beliebige Anzahl an Projekten verwalten. Jedes Projekt setzt sich aus einer Stammansicht und einer beliebigen Anzahl untergeordneter Ansichten zusammen. Die Stammansicht und alle untergeordneten Ansichten verfügen über jeweils einen Anwendungsordner als Stammordner. Jedem Stammordner einer Anwendung kann eine beliebige Hierarchie von Ordnern untergeordnet sein. Dies wird als Ordnerhierarchie bezeichnet. Wenn ein Administrator ein Projekt erstellt, werden seine Stammansicht und der Stammordner der Stammansicht automatisch erstellt und beide erhalten denselben Namen wie das Projekt. Wenn das Projekt beispielsweise den Namen *Super-Anwendung* hat, lautet der Name der Stammansicht und der Name des Stammordners anfänglich ebenfalls *Super-Anwendung* (obwohl der Administrator diese Namen ändern kann).

Ihre erste Aufgabe als Administrator besteht darin, den Server zu installieren, zu konfigurieren und zu registrieren. Dies wird im StarTeam-Installationshandbuch erläutert. Als Nächstes müssen Sie auf dem Computer, auf dem der

Server installiert ist, eine Instanz erstellen (diese wird als Serverkonfiguration bezeichnet). Eine Serverkonfiguration muss ausgeführt werden, bevor Sie oder Ihre Teammitglieder auf die Anwendung zugreifen können.

Verwandte Konzepte

Übersicht über die Serverkonfiguration
E-Mail-Unterstützung und angepasste E-Mail-Benachrichtigungen

Verwandte Verfahrensweisen

Server lizenzieren
Serverkonfigurationen erstellen
Benutzer und Gruppen verwalten
Unterstützung für Verzeichnisdienst aktivieren
Passwörter verwalten
Zugriffsrechte und Gruppenberechtigungen verwalten
Fehlerbehebung bei Problemen mit der Serverkonfiguration

Voraussetzungen für die Serveradministration

Serveradministratoren sollten mit dem Folgenden vertraut sein:

- Erstellen und Ändern von relationalen Datenbanken.
- Arbeiten mit den Funktionen ihres Betriebssystems, z. B. das Erstellen von Dateien, das Starten von ausführbaren Dateien und das Verwalten von Zugriffsrechten.
- Grundlegende Konzepte des Software-Konfigurationsmanagements.

In diesem Handbuch wird außerdem vorausgesetzt, dass Serveradministratoren Folgendes beachten:

- Datenbankinhalte dürfen ausschließlich mithilfe eines Clients oder mit dem Serveradministrations-Tool geändert werden. Bitte beachten Sie, dass die **direkte Datenbankmanipulation nicht unterstützt wird**.
- Datenspeicherdateien dürfen ausschließlich mithilfe eines Clients oder mit dem Serveradministrations-Tool geändert werden.

Verwandte Konzepte

Übersicht über die Serverkonfiguration
E-Mail-Unterstützung und angepasste E-Mail-Benachrichtigungen

Verwandte Verfahrensweisen

Server lizenzieren
Serverkonfigurationen erstellen
Benutzer und Gruppen verwalten
Unterstützung für Verzeichnisdienst aktivieren
Passwörter verwalten
Zugriffsrechte und Gruppenberechtigungen verwalten
Fehlerbehebung bei Problemen mit der Serverkonfiguration

Übersicht über die Serverkonfiguration

Vor der Verwendung des Servers müssen Sie entscheiden, mit welcher Datenbank Sie arbeiten möchten und wo die Datenbank und die Dateirevisionen gespeichert werden sollen. Anschließend müssen Sie mindestens eine Serverkonfiguration (eine Instanz des Servers) erstellen. In diesem Thema werden Serverkonfigurationen und ihre Speicher-*Hives* beschrieben.

Serverkonfigurationen

In einer Serverkonfiguration wird Folgendes gespeichert:

- Optionen wie die für den Serverzugriff verwendeten Endpunkte (der TCP/IP-Port) und Verschlüsselungsstufen.
- Der Speicherort der Datenbank, in der Projektdaten, der Datenbank-DSN und andere verwandte Informationen gespeichert sind.
- Die Speicherorte des Repositorys und der Ordner, die sich im Repository befinden

In einer Datenbank, die einer bestimmten Serverkonfiguration zugeordnet ist, kann eine beliebige Anzahl von Projekten gespeichert werden. Die Datenbank muss jedoch ordnungsgemäß konfiguriert sein, damit die von diesen Projekten erzeugte Datenmenge gespeichert werden kann. Weitere Informationen zu den von StarTeam unterstützten Datenbanken finden Sie im StarTeam-Installationshandbuch (Install_de.pdf).

Mithilfe des Dienstprogramms "Serveradministration" können Sie eine Serverkonfiguration erstellen. In einer Serverkonfiguration wird eine bestimmte Datenbank als Daten-Repository angegeben. Um Fehler zu vermeiden, kann eine Datenbank nur einer Serverkonfiguration zugeordnet werden. Sie kann jedoch von mehreren Anwendungen verwendet werden. Die Anwendung speichert alle Projekte auf dem Server, auf dem eine Vielzahl von Serverkonfigurationen bereitgestellt werden können.

Um auf ein vorhandenes Projekt zuzugreifen, müssen Sie zunächst seine Serverkonfiguration zu Ihrem System hinzufügen. Der Zugriff auf einen Server kann über den Cross-Platform-Client und den Web-Client erfolgen. Jeder Client muss über einen Benutzernamen und die benötigten Zugriffsrechte für die ausgewählte Serverkonfiguration verfügen. Die Daten Ihres Unternehmens oder Ihres Teams können in mehreren Serverkonfigurationen auf mehreren Computern gespeichert werden. Sie können von verschiedenen Clients aus auf diese Konfigurationen zugreifen.

Auf demselben Computer können mehrere Instanzen des Servers ausgeführt werden. Benutzer können beispielsweise eine Serverkonfiguration mit dem StarDraw-Beispielprojekt und eine weitere Konfiguration mit einem Softwareentwicklungsprojekt auf demselben Computer ausführen. Die Serverkonfigurationen haben unterschiedliche Namen und verwenden unterschiedliche Ports oder Endpunkte für jedes Protokoll. Wenn eine Konfiguration aktiv ist, kann keine weitere Sitzung mit dieser Konfiguration gestartet werden.

Vor dem Erstellen einer Serverkonfiguration müssen Sie einen eindeutigen Namen für die Konfiguration festlegen. Bei diesem Namen wird die Groß-/Kleinschreibung ignoriert. Der Name darf keine Doppelpunkte (:) sowie normale (/) oder umgekehrte (\) Schrägstriche enthalten. Leerzeichen oder Apostrophe (') sind jedoch zulässig.

Der Server legt die Serverprotokolldateien an der Position ab, die als Repository-Pfad der Serverkonfiguration angegeben wurde. Wenn Sie eine neue Serverkonfiguration das erste Mal starten, erstellt der Server am selben Speicherort die Ordner "Attachments", "HiveIndex" und weitere Ordner. Diese Ordner werden durch den Server verwaltet. Löschen Sie sie nicht.

Tipp: Wenn Sie eine Serverkonfiguration erstellt haben, können Sie den Pfad zum Ordner "Attachments" im Dialogfeld **Server konfigurieren** des Dienstprogramms "Serveradministration" ändern.

Über andere Serverkonfigurationseinstellungen wird gesteuert, welche Personen wann, wie und wo auf die Daten zugreifen dürfen. Bei einigen der anfänglichen Einstellungen, die Sie für die Serverkonfiguration festlegen, handelt es sich um notwendige Eigenschaften zum Starten des Servers. Wenn der Benutzername und das Passwort, mit

denen der Server versucht, auf die Datenbank zuzugreifen, nicht korrekt sind, kann der Server nicht ausgeführt werden. Vor dem Starten des Servers können Sie diese Eigenschaften ändern und an Ihre Anforderungen anpassen.

Native-II-Datenspeicher und Hives

Die neue Datenspeicher-Architektur (Native-II), die mit StarTeam 2005 eingeführt wurde, bietet größere Skalierbarkeit für alle Serverkonfigurationen ab StarTeam Version 2005 und Serverkonfigurationen, die mit StarTeam-Server 2005 oder höher in das Native-II-Datenspeicherformat konvertiert wurden. Serverkonfigurationen zeichnen sich dadurch aus, dass sie über mehrere *Hives* verfügen. Ein Hive ist ein logisches Dateisystem mit einem *Archiv*- und einem *Cache-Bereich*. Der *Archivbereich* umfasst einen Ordnerbaum, in dem eindeutige Dateirevisionen gespeichert werden. Der *Cache-Bereich* umfasst einen Ordnerbaum, in dem unkomprimierte Dateirevisionen temporär gespeichert werden. Hives können eine unbegrenzte Anzahl an Dateien enthalten, ermöglichen eine erhöhte Speicherkapazität, größere Dateirevisionen, mehr Speicherorte zum Speichern von Archiven sowie eine schnellere und effizientere Leistung. Eine einzelne Serverkonfiguration kann über mehrere Hives verfügen, wobei jeder dieser Hives einen eigenen Archiv- und Cache-Pfad besitzt.

Hinweis: StarTeam unterstützt nur das Native-II-Datenspeicher-Format für Hives.

Zusammen mit der Serverkonfiguration wird ein Hive für die Speicherung der Archivdateien der Serverkonfiguration eingerichtet. Sie müssen beim Erstellen der Serverkonfiguration einen Archiv- und einen Cache-Pfad zu diesem Hive angeben. Die vorgegebenen Pfade lauten `Repository_Pfad\DefaultHive\Archives` und `Repository_Pfad\DefaultHive\Cache`. Bei Bedarf können die Speicherorte dieser Pfade später über das Dialogfeld **Hive-Manager** im Dienstprogramm "Serveradministration" geändert werden.

Native-II-Datenspeicher speichern komplette Dateirevisionen (auch wenn die Archivdatei komprimiert ist). Diese Revisionen können jedoch mithilfe der Hive-Speicherung auf mehrere Volumes verteilt werden. Wenn ein Hive voll ist, können Sie einen weiteren hinzufügen, ohne die Speicherorte von Daten zu ändern oder Archivdateien verschieben zu müssen. Wenn eine Serverkonfiguration über mehrere Hives verfügt, fügt der Server den einzelnen Hives die Dateien abwechselnd hinzu, bevor er wieder den Archivpfad des ersten Hives verwendet. Weitere Informationen zu Native-II-Datenspeichern finden Sie im StarTeam-Installationshandbuch (Install_de.pdf).

Serverkonfigurationen, die mit StarTeam 2005 oder höher erstellt werden, verfügen automatisch über mindestens einen Hive (vorgegeben oder benutzerdefiniert). Um den für diese Serverkonfiguration verfügbaren Speicherplatz zu erweitern, können weitere neue Hives mithilfe des Hive-Managers hinzugefügt werden. Hives können während der Ausführung der Serverkonfiguration erstellt werden, da die Konfiguration bereits über einen anfänglichen Pfad verfügt, selbst wenn er nur auf einen vorgegebenen Hive im Repository-Pfad verweist. Der Hauptzweck des Hive-Managers ist es, neue Hives für eine vorhandene 2005- oder höhere Serverkonfiguration zu erstellen, um die Menge des verfügbaren Speicherplatzes zu erhöhen.

Verwandte Konzepte

Speicherorte für die Datenspeicherung

Verwandte Verfahrensweisen

Serverkonfigurationen erstellen
Optionen für die Datenspeicherung konfigurieren
Mit Serverkonfigurationen arbeiten

Richtlinien für die Serverkonfiguration

Im Rahmen der anfänglichen Planung besteht eine der wichtigsten Entscheidungen, die Ihre Organisation treffen muss, darin, wie viele StarTeam-Konfigurationen verwendet werden sollen. Das Verteilen von Projekten auf mehrere StarTeam-Server führt zwar zu höheren Verwaltungskosten, gleichzeitig erhöht es jedoch auch die Projektunabhängigkeit und verbessert die Leistung und die Verfügbarkeit. Indem Sie das Projektwachstum abschätzen und Wechselbeziehungen im Voraus berücksichtigen, können Sie das Aufteilen/Teilen von zu umfangreich gewordenen Konfigurationen vermeiden. Im Folgenden finden Sie einige Strategien, die Sie bei der Entwicklung des Serverbereitstellungsplans für Ihre Organisation berücksichtigen sollten.

Vorteile gemeinsam genutzter Serverkonfigurationen

Dies sind die Vorteile einer gemeinsamen Konfiguration, die von mehreren Projekten genutzt wird:

- **Transaktionale Integrität:** Da eine Konfiguration eine einzige Datenbank verwendet, sind alle Daten innerhalb derselben Konfiguration *transaktional* konsistent. Das bedeutet, dass eine Konfiguration eine Begrenzung für die Datenkonsistenz darstellt. Wenn Sie eine Konfiguration sichern und später wiederherstellen, werden alle Informationen innerhalb der Konfiguration für denselben Zeitpunkt wiederhergestellt.
- **Verknüpfen:** Elemente innerhalb derselben Konfiguration können miteinander verknüpft werden, auch dann, wenn sie sich in verschiedenen Projekten befinden. StarTeam unterstützt derzeit keine Verknüpfungen zwischen Elementen in verschiedenen Konfigurationen.
- **Freigeben und verschieben:** Elemente können freigegeben oder in einen beliebigen Ordner, eine Ansicht oder ein Projekt innerhalb derselben Konfiguration verschoben werden. Das Verschieben oder Freigeben von Elementen über Konfigurationsgrenzen hinweg wird nicht unterstützt.
- **Einfache Administration:** Administrative Tasks wie das Hinzufügen von Benutzern und Gruppen, das Anwenden von Sicherheitsmaßnahmen, das Durchführen von Backups usw. werden auf der Konfigurationsebene ausgeführt.
- **Gemeinsam genutzte Anpassungen:** Viele StarTeam-Ressourcen, wie z. B. Filter, Abfragen, benutzerdefinierte Formulare und Workflows, können auf der Konfigurationsebene definiert und von allen Projekten gemeinsam verwendet werden. (Benutzerdefinierte Formulare und Workflows können jedoch auch für einzelne Projekte oder Ansichten angepasst werden.)
- **Gemeinsam genutzte Serverkomponenten:** Alle Daten innerhalb derselben Konfiguration verwenden einen einzigen Serverprozess, eine Datenbank, einen Datenspeicher und einen Root-Cache-Agent. Neue Projekte können dynamisch hinzugefügt werden, ohne dass neue serverseitige Komponenten hinzugefügt werden.

Vorteile separater Serverkonfigurationen

Dies sind die Vorteile der Verwendung von separaten Konfigurationen für mehrere Projekte:

- **Leistung:** Bei größeren Konfigurationen dauert der Startvorgang länger, sie benötigen mehr Ressourcen und sie geben häufig umfangreichere Antworten auf Befehle zurück. Bei kleineren Konfigurationen dagegen sind weniger Daten und weniger gleichzeitige Benutzer vorhanden, daher ist ihre Leistung im Hinblick auf diese Aspekte normalerweise besser.
- **Wachstumsverwaltung:** Auch wenn Sie anfänglich mehrere Konfigurationen auf einem einzelnen Rechner platzieren, können Sie bei Bedarf einfach eine Konfiguration auf den entsprechenden Rechner verschieben.
- **Wartungsplanung:** Separate Konfigurationen können unabhängig voneinander gestartet und gestoppt werden, um Patches zu installieren, Hardware zu aktualisieren usw. Wenn eine Konfiguration offline ist, kann auf keine der darin enthaltenen Projekte zugegriffen werden.
- **Benutzerdefinierte Felder:** Benutzerdefinierte Felder werden auf der "Typ"-Ebene hinzugefügt, die den Gültigkeitsbereich der Konfigurationsebene besitzt. Dies bedeutet, dass wenn Sie ein benutzerdefiniertes Feld zu einer Änderungsanforderung hinzufügen, alle Änderungsanforderungen in der jeweiligen Konfiguration einen Wert für das Feld besitzen. Wenn daher verschiedene Teams oder Geschäftsbereiche im Hinblick auf

benutzerdefinierte Felder unterschiedliche Interessen haben, spricht dies dafür, deren Projekte in separate Konfigurationen zu platzieren.

Weitere Überlegungen zu Serverkonfigurationen

Im den folgenden Abschnitten werden zusätzliche Faktoren beschrieben, die Sie bei der Entwicklung des Serverbereitstellungsplans für Ihre Organisation berücksichtigen sollten.

Einteilungen in Geschäftsbereiche

Wenn mehrere Geschäftsbereiche ihre eigenen StarTeam-Projekte benötigen, bietet es sich in der Regel an, die StarTeam-Server gemäß diesen organisationsspezifischen Bereichen zu definieren. Dies bedeutet, dass Sie pro Geschäftsbereich oder Abteilung einen separaten StarTeam-Server bereitstellen, sodass diese auf ihre eigenen Projekte zugreifen können. Durch das Aufteilen der Server nach Geschäftsbereichen werden die separaten (und gelegentlich konkurrierenden) Anforderungen für Sicherheit, Backup-Prozesse und andere administrative Punkte isoliert. Separate Server können auch helfen, Probleme mit Eigentumsrechten zu minimieren.

Wenn Prozesse des Entwicklungslebenszyklus sich über mehrere Serverkonfigurationen erstrecken, können auf einem einzelnen StarTeam-Client mehrere Projekte geöffnet werden. Um konfigurationsübergreifenden Anforderungen zu entsprechen, kann auch das "Bereitstellen" zusammenhängender Artefakte von einem Projekt in ein anderes verwendet werden.

Optimierte StarTeam-Unterstützung für verteilt arbeitende Teams

Teammitglieder, die Zugriff auf dieselben Artefakte benötigen, sollten einen StarTeam-Server gemeinsam nutzen. Das Aufteilen eines StarTeam-Servers nur aus dem Grund, dass sich die Teammitglieder an verschiedenen Standorten befinden, ist nicht erforderlich. StarTeam ist darauf ausgelegt, dass die Arbeit mit Teams, deren Mitglieder sich an verschiedenen Orten befinden, gut funktioniert. In StarTeam wird Wert auf einen zentralisierten Konfigurationsansatz mit MPX-Publish/Subscribe-Messaging und Cache-Agenten gelegt, um geografisch verteilte Teams zu unterstützen.

Vermeidung von Partitionen für den internen/externen Zugriff

In vielen Situationen benötigen Teams sowohl hinter als auch außerhalb der Unternehmens-Firewall Zugriff auf dieselbe StarTeam-Konfiguration. In diesem Szenario wird der StarTeam-Serverprozess in der Regel im DMZ-Bereich der Firewall bereitgestellt und der Datenbankserver und der Speicherserver werden hinter der Firewall platziert. Je nach Funktionalität der Firewall kann es angebracht sein, einen dedizierten Port für den StarTeam-Server zu konfigurieren. Alternativ können Sie auf dem StarTeam-Server-Computer auch zwei Netzwerkkarten (NICs) installieren: eine für die externe und eine für die interne Kommunikation. In diesem Szenario ermöglicht StarTeam, dass bestimmte IP-Adressen (oder Adressbereiche) für den eingehenden Verkehr mit unterschiedlichen Anforderungen für die Verbindungssicherheit konfiguriert werden können.

StarTeam bietet eine SSL-ähnliche Verschlüsselung für die Befehls-API, um das Abhören von Client/Server-Traffic zu verhindern. Der gesamte MPX Message Broker- und Cache-Agent-Verkehr ist ebenfalls verschlüsselt, sodass Daten, die über öffentliche Verbindungen übermittelt werden, nicht öffentlich zugänglich sind. Wenn Sie den Zugriff auf bestimmte Teams beschränken möchten, können Sie Referenzansichten oder die Sicherheits-ACLs von StarTeam dazu verwenden, den Zugriff auf bestimmte Projekte, Ansichten, Ordner und sogar einzelne Artefakte zu beschränken. Weitere Sicherheitsfunktionen, z. B. die Verwaltung sicherer Passwörter und automatische Kontensperren, können die Sicherheit der Verwendung derselben StarTeam-Konfiguration sowohl für interne als auch für externe Benutzer weiter erhöhen.

Für Wachstum planen

Bei der Überlegung, wie viele StarTeam-Konfigurationen Sie erstellen möchten, sollten Sie für einen längeren Zeitraum im Voraus planen: mindestens für drei bis fünf Jahre. Wenn Sie die gleichzeitige Nutzung durch mehrere

Benutzer abschätzen können, stellt dies den besten Maßstab für die Kapazitätsplanung dar. Auf der heutigen Hardware (Vierfach-CPU mit 4 GB Arbeitsspeicher) unterstützt StarTeam ohne Schwierigkeiten bis zu 300 gleichzeitige Benutzer. Einige Kunden besitzen Konfigurationen, bei denen die maximale Anzahl von gleichzeitigen Benutzern bei über 400 liegt, und bei einem Kunden sind es zeitweilig sogar 600 gleichzeitige Benutzer. Bei diesen Mengen von gleichzeitigen Benutzern kommt jedoch den Anwendungstypen eine Bedeutung zu (beispielsweise sind bei Stapelanwendungen normalerweise die Anforderungen höher als bei Online-Clients). Selbst bei 300 gleichzeitigen Benutzern kann sich die Leistung in nicht akzeptablem Maße verringern, wenn eine große Anzahl von Benutzern Anwendungen ausführen, die hohe Anforderungen stellen.

Die Skalierbarkeit von Konfigurationen kann auch mit Befehlsraten gemessen werden. Sie können die Befehlsraten einer vorhandenen Konfiguration mithilfe der Server-Trace-Funktionalität messen. Der StarTeam-Server kann so eingestellt werden, dass er bei Befehlsraten zwischen 200.000 und 300.000 Befehlen pro Stunde (56 bis 83 Befehle pro Sekunde) eine angemessene Performance bietet. Bei guter Netzwerk-Infrastruktur (niedrige Latenz) wurden bereits Befehlsraten von 400.000 Befehlen pro Stunde (111 Befehle pro Sekunde) und mehr bei angemessener Performance erreicht. Wenn versucht wird, bei einer einzelnen Konfiguration höhere Werte zu erzielen, entstehen zumeist inakzeptable Antwortzeiten.

Wenn es Ihnen nicht möglich ist, die Anzahl der gleichzeitigen Benutzer oder die Befehlsraten vorauszuberechnen, können Sie "definierte" Benutzer verwenden. Die Serverauslastung ist bei der alleinigen Verwendung von definierten Benutzern jedoch schwieriger vorherzusagen. Wenn sich die Benutzer einer Benutzergruppe an unterschiedlichen Standorten befinden, liegt das Verhältnis von definierten Benutzern zu gleichzeitigen Benutzern in der Regel bei etwa 10:1. Bei 1.000 benannten Benutzern ist demnach zu Spitzenzeiten mit etwa 100 gleichzeitigen Benutzersitzungen zu rechnen. Wenn die Standorte der Benutzer weniger variieren und die Benutzer in einer oder zwei Zeitzonen konzentriert sind, ist zu erwarten, dass das Verhältnis von definierten Benutzern zu gleichzeitigen Benutzern eher bei etwa 5:1 liegt. Wenn Ihnen keine besseren Daten zur Verfügung stehen, verwenden Sie diese Näherungswerte, um die Anzahl von gleichzeitigen Benutzern zu Spitzenzeiten zu bestimmen.

Nachdem Sie Ihre Vorhersage für die nächsten drei bis fünf Jahre berechnet haben, sollten Sie einschätzen können, wie viele StarTeam-Konfigurationen für Ihren Benutzerkreis erforderlich sein werden.

Verwandte Konzepte

Übersicht über die Serverkonfiguration

Verwandte Verfahrensweisen

Serverkonfigurationen erstellen
Dateirevisionen mit Vault Verify verifizieren
Gelöschte Ansichten aus Serverkonfigurationen entfernen

Audit-Protokolle

Der Server wird standardmäßig für das Generieren von Audit-Protokollen konfiguriert. Wenn diese Option aktiviert ist, protokolliert der Server Audit-Ereignisse für Projekte in der Datenbank für die Serverkonfiguration. Im Protokoll wird beispielsweise aufgezeichnet, wann Änderungsanforderungen erstellt und Dateien hinzugefügt werden. Die Einträge des Audit-Protokolls werden im Client angezeigt, wenn Sie im oberen Teilfenster das Register "Audit" auswählen. Diese Operation kann nur bei einer gestarteten Serverkonfiguration ausgeführt werden.

Das Audit-Protokoll ist eine chronologische Aufzeichnung, in der Daten über die mit Ordnern, Dateien, Anforderungen, Änderungsanforderungen, Tasks und Themen ausgeführten Aktionen gesammelt werden. Jeder Protokolleintrag enthält folgende Informationen: Benutzer, der die Aktion ausgeführt hat, Datum und Uhrzeit der ausgeführten Aktion, Klassenname (Elementtyp), Ereignis (Aktionstyp) und Ansichts- und Projektname. Sie können nach allen Einträgen für ein bestimmtes Element suchen, indem Sie Filter oder Abfragen verwenden.

Folgende Ereignisse stehen für die meisten Elemente zur Verfügung: "Hinzugefügt", "Verzweigt", "Kommentar", "Erstellt", "Gelöscht", "Geändert", "Verschoben von", "Verschoben nach" und "Gemeinsam genutzt". Bei Dateien stehen zusätzlich Ereignisse zur Verfügung, die über die Konvertierung, die Bearbeitung, überschriebene Elemente, Sperren, umgangene Sperren und nicht gesperrte Elemente informieren. Protokolleinträge an sich können nicht entfernt, gemeinsam genutzt, geändert oder verzweigt werden. Wenn im Register "Audit" des Hauptfensters keine Einträge angezeigt werden, hat Ihr Administrator die Audit-Protokollfunktion möglicherweise deaktiviert.

Verwandte Verfahrensweisen

Das Audit-Protokoll aktivieren und bereinigen

StarDraw (Beispiel-Serverkonfiguration)

StarTeam stellt eine Beispiel-Serverkonfiguration mit dem Namen "StarDraw" bereit. Diese enthält eine Beispielanwendung in Visual C++ und ähnliches Material. Zudem bietet sie Beispieldateien, Änderungsanforderungen, Themen und Tasks. Sie enthält zudem das StarFlow Extensions-Projekt. Weitere Informationen hierzu finden Sie im StarTeam-Einführungshandbuch. Mithilfe des Beispiel-Repositorys können Sie experimentieren und sich mit StarTeam vertraut machen.

Ab StarTeam Server 2009 erstellt der Server neue Projekte, bei denen nur der Typ "Datei" als Vorgabe für neue Ansichten vorab ausgewählt ist. Benutzer können die Projekteigenschaften nach wie vor nach Erstellen des Projekts ändern und sie können auch die aufgenommenen Elementtypen für eine neue Ansicht ändern. Wenn allerdings der Benutzer nichts ändert, enthalten neue Ansichten nur dann standardmäßig Dateien, wenn sie erstellt werden.

Hinweis: Diese Änderung wirkt sich nicht auf vorhandene Projekte aus. Sie betrifft nur neue Projekte, die mit StarTeam Server 2009 oder vorhandenen Servern, die auf StarTeam Server 2009 aktualisiert wurden, erstellt wurden. Durch das Hinzufügen von anderen Elementtypen zu den Projekteigenschaften (nachdem die Ansicht erstellt wurde) wird die Ansicht NICHT mit den Elementen gefüllt, die in der übergeordneten Ansicht enthalten waren (aber während des Erstellens der neuen Ansicht übergangen wurden). Falls der Benutzer die vorherigen Elemente in die neue Ansicht aufnehmen möchte, muss er sie abrufen, indem er die Basis von der übergeordneten Ansicht ändert.

Die Beispiel-Serverkonfiguration ist Bestandteil der Standardinstallation von StarTeam-Server und kann bei der benutzerdefinierten Installation ausgewählt werden. Während des Installationsvorgangs geschieht Folgendes:

- Die Datenbank `stardraw.mdf` wird im Ordner `StarTeam Server 2009\Samples\StarDraw Repository\Database` abgelegt.
- Kopiert Beispieldateien in den Ordner `StarTeam Server 2009\Samples\StarDraw Repository\StarDraw\Archives` und dessen Unterordner.
- Es wird ein ODBC-System-DSN (Data Source Name) mit dem Namen `StarDrawDB110` erstellt.
- Das System fügt die neue StarDraw-Serverkonfiguration zur Datei "starteam-server-configs.xml" hinzu. Wenn in der Datei bereits eine StarDraw-Serverkonfiguration vorhanden ist, werden die Einstellungen auf die StarDraw-Konfiguration der neuen Version aktualisiert.

Hinweis: In der Datei `starteam-server-configs.xml` lautet der vordefinierte Wert von `ServerGuid` für das StarDraw-Repository wie folgt:

be5ee3b0-c719-49c6-a1a1-f493764a03f5

Ändern Sie diesen Wert nicht. Die StarDraw-Serverkonfiguration kann nicht gestartet werden, wenn Sie den ServerGuid-Wert ändern. Verwenden Sie die StarDraw-Serverkonfiguration nur zum Experimentieren und für Schulungszwecke – niemals für echte Daten.

Verwandte Verfahrensweisen

Das Audit-Protokoll aktivieren und bereinigen

Einführung in die Benutzeroberfläche

Dieser Abschnitt enthält konzeptionelle Themen, die sich auf die StarTeam-Benutzeroberfläche beziehen.

In diesem Abschnitt

Serveradministrations-Tool
Dieses Thema beschreibt die Benutzeroberfläche des Serveradministrations-Tools.

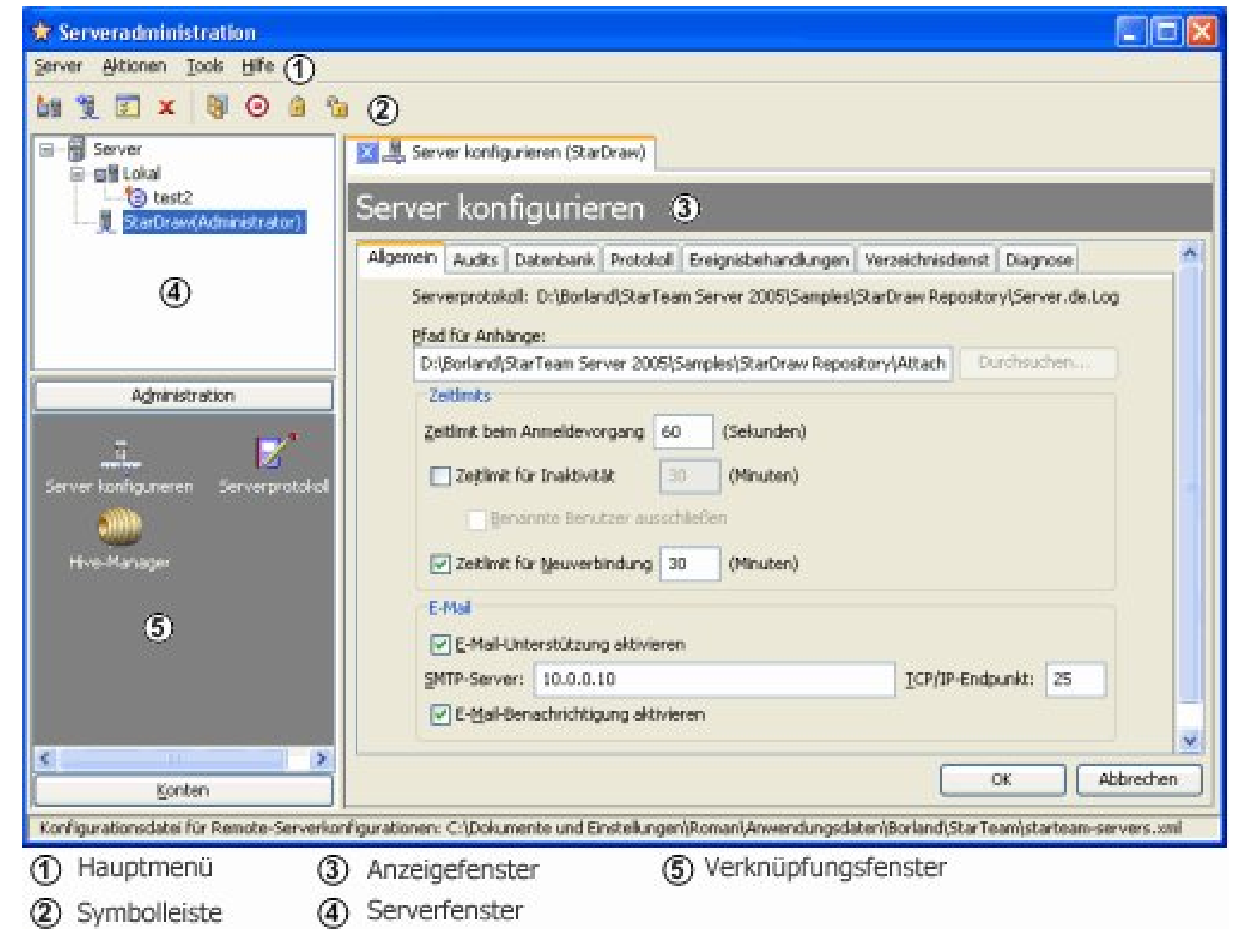
VCM anpassen
Dieses Thema beschreibt das "Customize VCM"-Tool, mit dem Administratoren benutzerdefinierte Typen für das Vergleichen/Zusammenführen von Ansichten erstellen können.

Online-Bereinigung
In diesem Thema wird die Benutzeroberfläche des Tools der Online-Bereinigung dargestellt, anhand der Administratoren gelöschte Ansichten und Daten auf einem laufenden Server bereinigen können.

Serveradministrations-Tool

Dieses Thema beschreibt die Benutzeroberfläche des Serveradministrations-Tools.

Benutzeroberfläche des Serveradministrations-Tools



Zum Verwalten der Serverkonfigurationen verwenden Sie das Serveradministrations-Tool. Das Serveradministrations-Toolist eine Java-Anwendung, mit der Administratoren Serverkonfigurationen und die zugehörigen Repositorys erstellen und verwalten können. Es wird zusammen mit dem StarTeam-Server automatisch installiert und kann nur auf dem Computer ausgeführt werden, auf dem der Server installiert ist. Es verwaltet serverseitig lokale und Remote-Konfigurationen, da es auf die Datei `starteam-server-configs.xml` zugreifen kann, die sich auf dem Server befindet.

Wenn Sie die benutzerdefinierte Installation ausführen, können Sie dieses Dienstprogramm auch mit dem Client installieren. Das Tool kann über den Client jedoch nur zur Verwaltung von Remote-Serverkonfigurationen eingesetzt werden. Das Serveradministrations-Tool ermöglicht Administratoren, die folgenden Operationen für lokale und Remote-Serverkonfigurationen auszuführen:

- Eine Serverkonfiguration erstellen, aktivieren, deaktivieren oder löschen.
- Die Sitzungsoptionen einer Serverkonfiguration anzeigen oder ändern.
- Eine Serverkonfiguration starten oder beenden.
- Eine Serverkonfiguration als Windows-Dienst einrichten oder als Anwendung ausführen.

- Den Status und den Ausführungsmodus aller auf diesem Computer ausgeführten Serverkonfigurationen überprüfen.
- Den Hive-Manager aufrufen.

Außerdem können die folgenden Aufgaben über Clients auf Remote-Serverkonfigurationen ausgeführt werden, auf denen das Serveradministrations-Tool installiert ist:

- Sich unter anderem Benutzernamen beim Server anmelden.
- Benutzerkonten hinzufügen und verwalten.
- Die Sicherheitsrichtlinie für eine Serverkonfiguration festlegen.
- Benutzern und Gruppen Zugriffsrechte für eine Serverkonfiguration zuweisen.
- Verbindungen mit einer Serverkonfiguration hinzufügen, bearbeiten oder löschen.
- Die Konfigurationsoptionen einer Serverkonfiguration festlegen oder ändern.
- Die Serverprotokolldatei anzeigen (`Server.locale.Log`).
- Serverkonfigurationen sperren oder entsperren.

Des Weiteren werden in diesem Thema die nummerierten Komponenten im obigen Diagramm beschrieben.

Hauptmenü

Das Hauptmenü besteht aus den Menüs **Server**, **Aktionen**, **Tools** und **Hilfe**. Das Menü **Tools** enthält weitere Menüs mit administrativen Befehlen und Befehlen für die Benutzerkonten.

Das Serveradministrations-Tool aktiviert bzw. deaktiviert Menübefehle je nach Status der Serverkonfiguration. Wenn Sie beispielsweise keine Serverkonfiguration ausführen, aktiviert das Serveradministrations-Tool die Hauptmenübefehle **Aktionen** ▸ **Anmeldung als StarTeam-Server herunterfahren** nicht.

Symbolleiste

Häufig verwendete Hauptmenübefehle, die den Menüs **Server** und **Aktionen** entsprechen, verfügen in der Symbolleiste über entsprechende Schalter. Wenn Sie den Mauszeiger über die Symbolleistenschalter halten, wird eine Kurzbeschreibung des jeweiligen Schalters angezeigt. Das Serveradministrations-Tool aktiviert bzw. deaktiviert die Symbolleistenschalter je nach Status der Serverkonfiguration.

Serverfenster

Im Serverfenster sind die Server aufgelistet, die in der Datei `starteam-servers.xml` enthalten sind. Wenn Sie **Server** ▸ **Server hinzufügen** wählen und die Optionen im Dialogfeld **Server hinzufügen** verwenden, wird diese Datei aktualisiert.

Fenster 'Verknüpfungen'

In diesem Fenster werden die Schalter für den Schnellzugriff angezeigt, die den kaskadierenden Menüs unter dem Menü **Tools** für die administrativen und benutzerkontospezifischen Befehle entsprechen. Das Verknüpfungsfenster ist in die Bereiche **Administration** und **Konten** aufgeteilt, in denen Sie auf häufig verwendete Hauptmenübefehle zugreifen können.

Anzeigefenster

Wenn Sie über das Menü "Tools" oder im Verknüpfungsfenster über die Schalter für den Schnellzugriff auf die Hauptmenübefehle zugreifen, zeigt Serveradministrations-Tool die Dialogfelder für die Befehle im Anzeigefenster an.

Tipp: Erweitern Sie das Serveradministrations-Tool-Fenster, um die im Anzeigefenster dargestellten Dialogfelder zu vergrößern.

Verwandte Konzepte

Wo befindet sich die Dokumentation für die einzelnen Produkte
StarTeam Produktübersicht

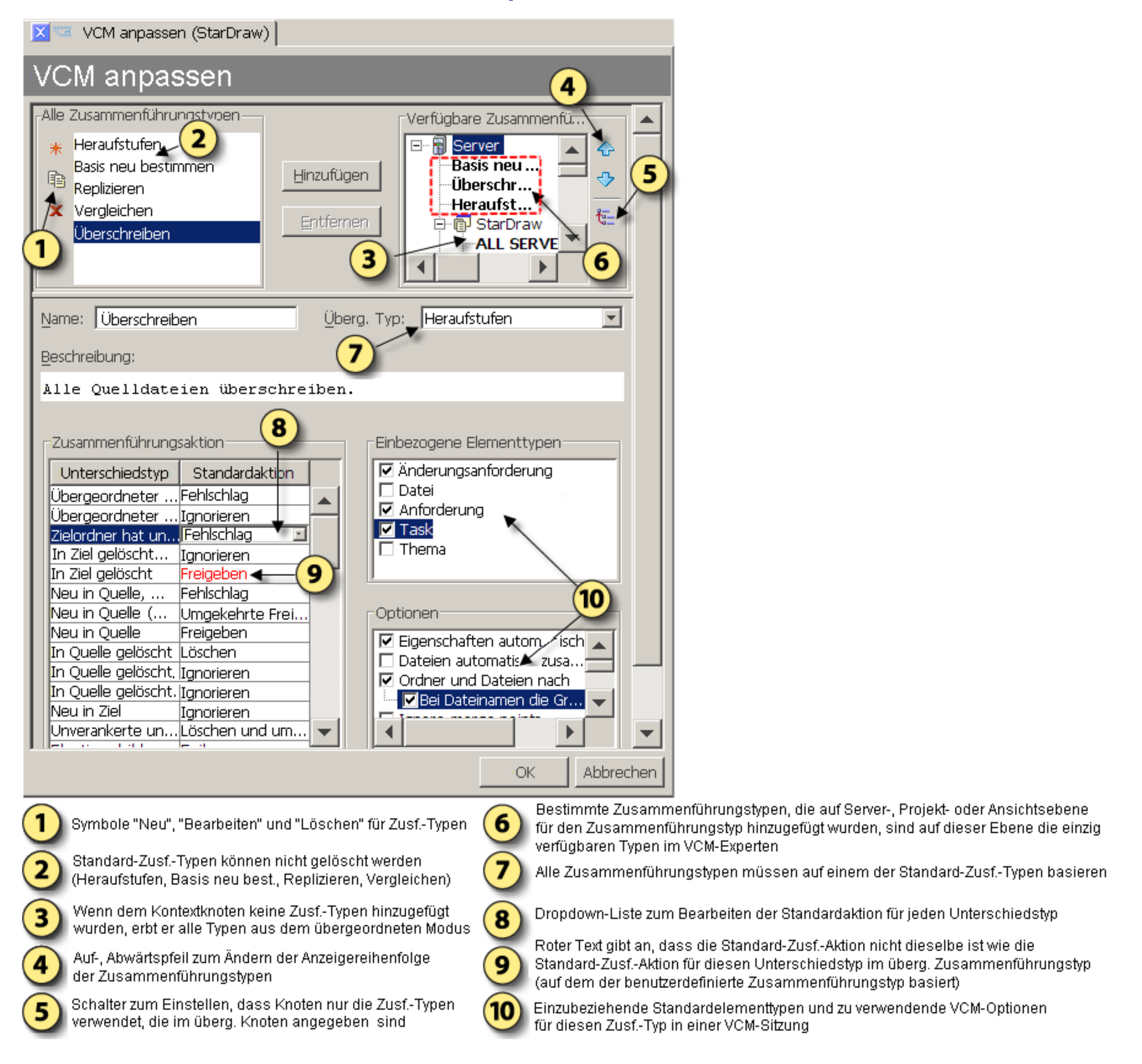
VCM anpassen

Mit dem Tool **VCM anpassen** im Fenster **Serveradministration** kann ein Administrator basierend auf den Standardzusammenführungstypen von "Basis neu bestimmen", "Heraufstufen", "Replizieren" und "Vergleichen" neue, benutzerdefinierte Typen für das Vergleichen/Zusammenführen von Ansichten erstellen. Auf Server-, Ansichts- oder auf Projektebene kann der Administrator angeben, welche Zusammenführungstypen dem Benutzer im jeweiligen Kontext zur Verfügung stehen. Der Administrator kann zudem die Standardzusammenführungsaktion für jeden Unterschiedstyp angeben, der in der Sitzung gefunden wird.

Der Einsatz des Tools **VCM anpassen** durch Administratoren vereinfacht den Vorgang des Vergleichens/ Zusammenführens von Ansichten, da die Einstellungen der VCM-Operationen im Experten **Ansichten vergleichen/ zusammenführen** vordefiniert sind, und es den Benutzern erspart bleibt, selbst alle Einstellungen begutachten und definieren zu müssen, um eine VCM-Sitzung starten zu können. Neben der Einstellung der Standardzusammenführungsaktion kann der Administrator auch angeben, welche **einbezogenen Elementtypen** und VCM-**Optionen** dem Benutzer bereitgestellt werden sollen.

Hinweis: Bevor Sie einen benutzerdefinierten VCM-Zusammenführungstyp erstellen können, müssen Sie auf dem Server ein StarFlow Extensions-Projekt erstellen. Erstellen Sie zuerst ein StarFlow Extensions-Projekt und anschließend den `Projects`-Ordner unterhalb des Stammordners der Ansicht. Anderenfalls führt der Speichervorgang im Tool **VCM anpassen** zu einem Fehler.

Benutzeroberfläche des Tools 'VCM anpassen'



Verfügbare Zusammenführungstypen

Der Administrator kann steuern, welche benutzerdefinerten Zusammenführungstypen in einem bestimmten Kontext (also auf Server-, Ansichts- oder Projektebene) zur Verfügung stehen. Das Tool **VCM anpassen** bietet einen hierarchischen Kontextbaum an, ausgehend vom Server selbst bis hinunter zu den Projekten und Ansichten auf dem Server. Auf jeder gewünschten Ebene des Kontextbaums können benutzerdefinierte Zusammenführungstypen hinzugefügt werden.

Im Baum mit den **verfügbaren Zusammenführungstypen**

- Bei den mit Symbolen versehenen Knoten handelt es sich um Kontextknoten, zu denen Server-, Projekt- und Ansichtsebenen gehören können.
- Die fett hervorgehobenen Knoten definieren, welche Zusammenführungstypen dem Benutzer im entsprechenden Kontext zur Verfügung stehen.

Wenn StarTeam in der aktuellen Ansicht keine Einstellungen für eine Funktion findet, wird standardmäßig in der übergeordneten Ansicht danach gesucht. Sind auch dort keine Einstellungen definiert, durchsucht StarTeam den Baum ebenenweise nach oben bis zur Serverebene. Wird einem Knoten ein benutzerdefinierter Zusammenführungstyp hinzugefügt, steht dieser in allen untergeordneten Knoten zur Verfügung.

Hinweis: Sobald Sie auf einer Ebene im Baum **Verfügbare Zusammenführungstypen** bestimmte Zusammenführungstypen hinzufügen, stehen nur die explizit hinzugefügten Zusammenführungstypen im Experten zum **Vergleichen/Zusammenführen von Ansichten** auf dieser Ebene für VCM-Sitzungen zur Verfügung. Sie müssen alle Standardzusammenführungstypen speziell auf dieser Ebene hinzufügen, wenn sie verfügbar sein sollen. Mit dem Schalter **Übergeordnete Zusammenführungstypen** können Sie eine Ebene schnell zurücksetzen, damit dort nur die ihr übergeordneten Zusammenführungstypen verwendet werden.

Im Experten **Ansichten vergleichen/zusammenführen** werden Zusammenführungstypen in der Reihenfolge angezeigt, in der Sie sie einer Kontextebene hinzugefügt haben. Sie können die Reihenfolge mit dem **Auf-** und **Abwärtspfeil** rechts neben dem Baum **Verfügbare Zusammenführungstypen** ändern.

Standardaktionen für Unterschiedstypen

In der Vergleichsphase einer Sitzung zum Vergleichen/Zusammenführen von Ansichten verwendet VCM die Standardzusammenführungsaktionen für den für die Lösung von Unterschieden ausgewählten Zusammenführungstyp. Der Serveradministrator kann steuern, welche Standardaktionen VCM für jeden Unterschiedstyp durchführt. Im Abschnitt **Zusammenführungsaktion** kann der Administrator die Standardaktion ändern, indem er aus den Dropdown-Listen in der Spalte **Standardaktion** eine andere Aktion auswählt.

Hinweis: Eine geänderte Zusammenführungsaktion, die von ihrer übergeordneten Standardaktion abweicht, wird in roter Textfarbe angezeigt.

Typen berücksichtigen

Der Benutzer kann die Elementtypen, die in einer VCM-Sitzung berücksichtigt werden sollen, auf der Seite **Ausgewählten Typ "Elemente" berücksichtigen** des Experten **Ansichten vergleichen/zusammenführen** begrenzen. Durch das Aktivieren bestimmter Elementtypen im Abschnitt **Typen berücksichtigen** des Tools **VCM anpassen** kann der Serveradministrator festlegen, welche Elementtypen dem Benutzer im Experten **Ansichten vergleichen/zusammenführen** zur Verfügung stehen.

Optionen

Im Abschnitt **Optionen** kann der Administrator angeben, welche Optionen zum Vergleichen/Zusammenführen auf der Seite zum **Festlegen der Optionen** des Experten zum **Vergleichen/Zusammenführen von Ansichten** standardmäßig angezeigt werden sollen. Die auf dieser Seite des Experten ausgewählten Optionen werden durchgeführt, wenn die Vergleichsphase der VCM-Sitzung beginnt.

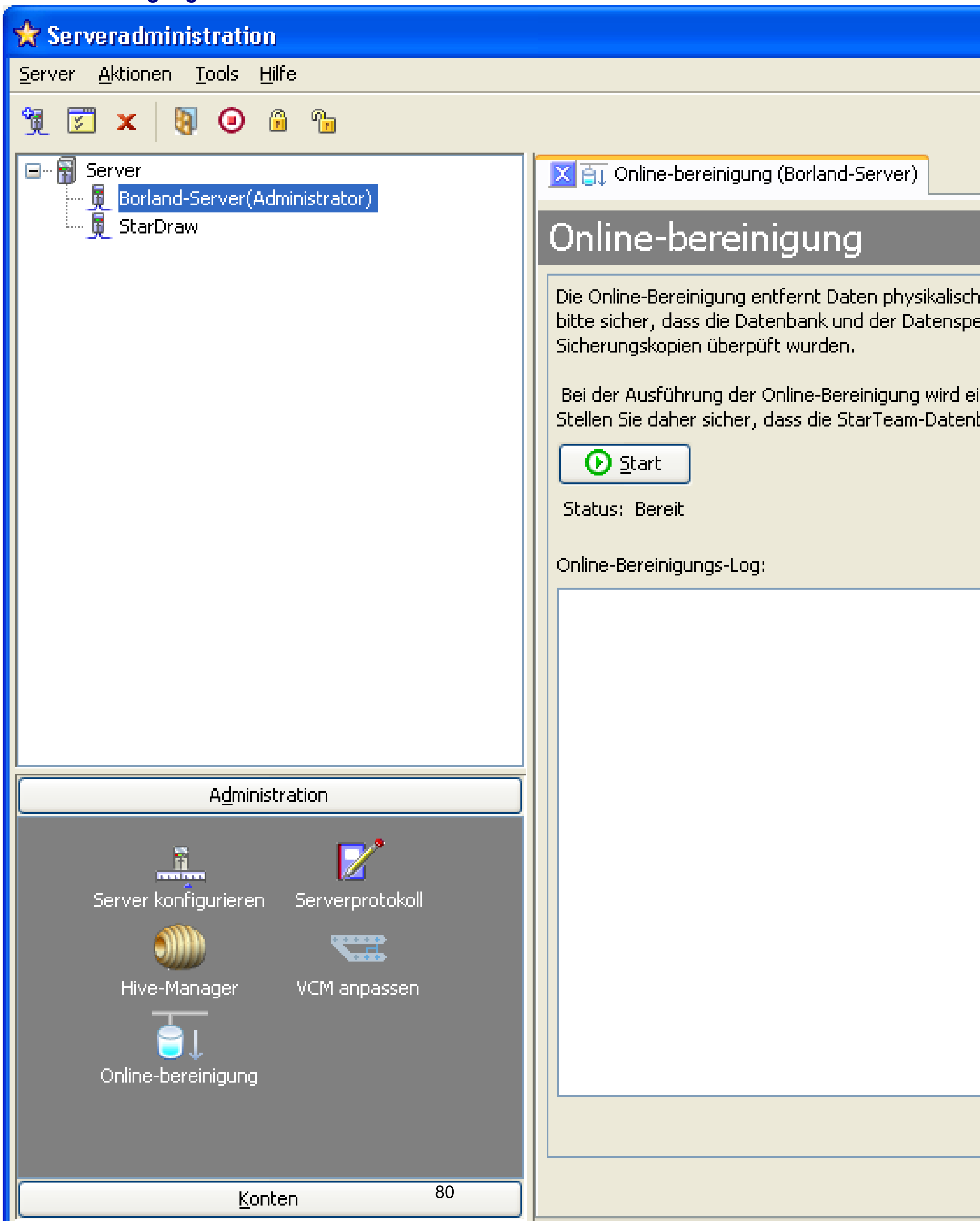
Online-Bereinigung

In diesem Thema wird die Benutzeroberfläche des Tools der Online-Bereinigung im Fenster **Serveradministration** dargestellt, anhand der Administratoren gelöschte Ansichten und Daten auf einem laufenden Server bereinigen können. Der Bereinigungsvorgang löscht unerwünschte Daten aus der Datenbank und entfernt gelöschte Archive aus dem Datenspeicher. Diese Operation kann nur bei aktivierter Serverkonfiguration ausgeführt werden.

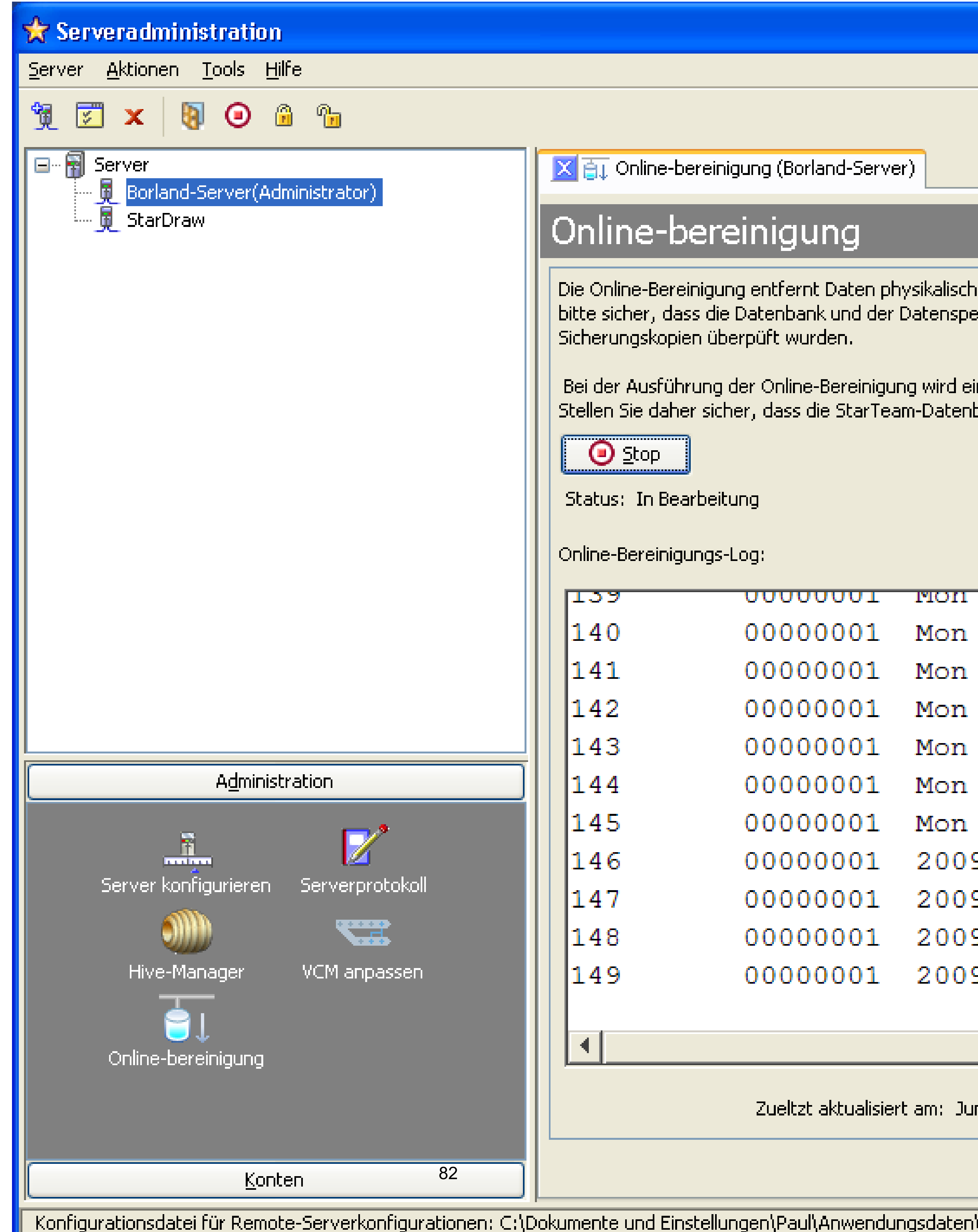
Das Tool der **Online-Bereinigung** enthält einen einfachen **Start/Stopp**-Schalter und ein Protokoll-Inhaltsfenster in der unteren Hälfte, in dem der Fortschritt der Bereinigung angezeigt wird. Diese Anzeige kann jederzeit aktualisiert werden.

Nachfolgend finden Sie Abbildungen der drei Stadien der Online-Bereinigung:

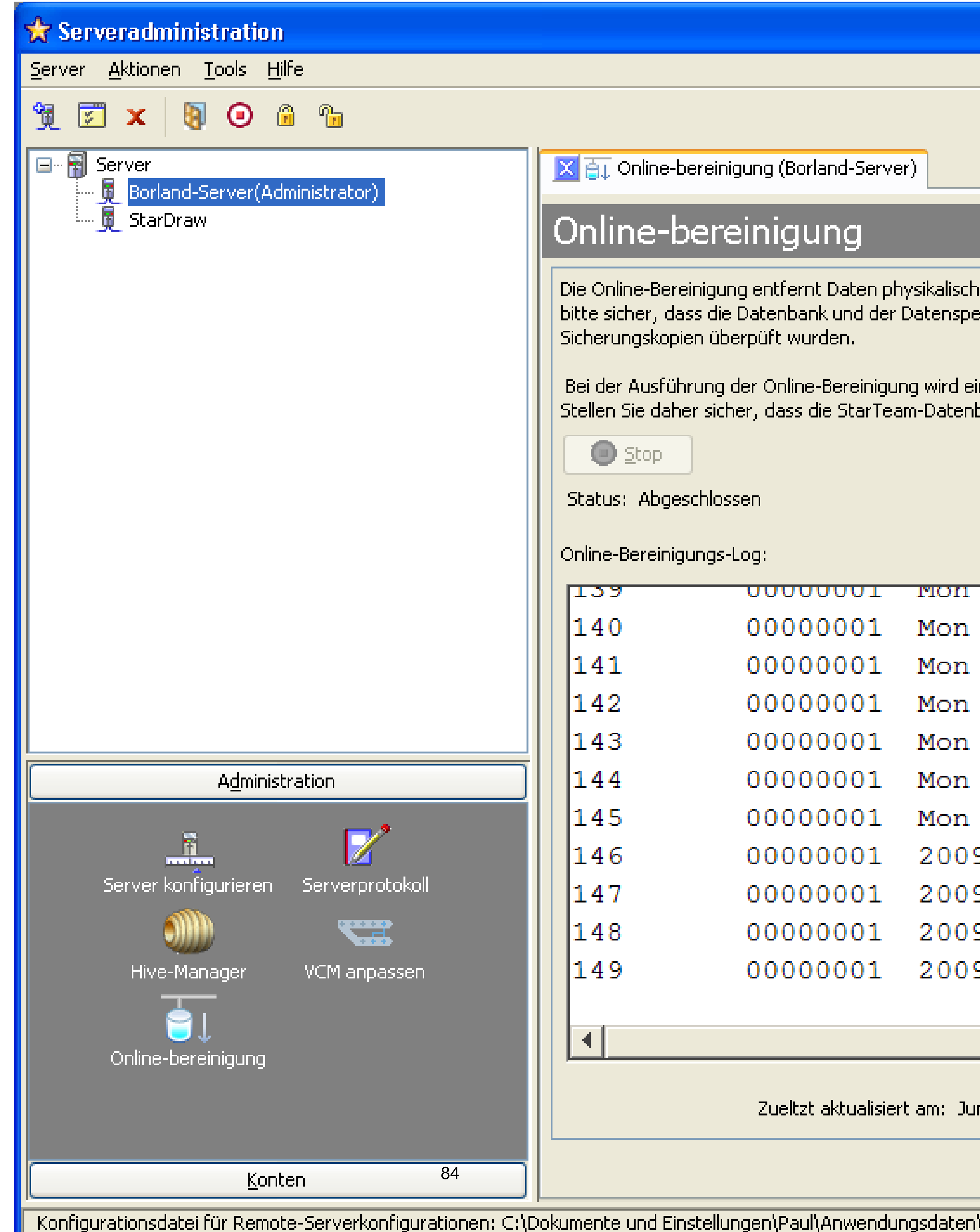
Online-Bereinigung - Startbereit



Online-Bereinigung - Wird verarbeitet



Online-Bereinigung - Abgeschlossen



Verwandte Konzepte

Online-Bereinigung

Verwandte Verfahrensweisen

Online-Bereinigen starten und stoppen

Konzepte

Dieser Abschnitt enthält alle konzeptionellen Themen.

In diesem Abschnitt

Serveradministration
Dieser Abschnitt enthält konzeptionelle Themen, die sich mit der Serveradministration befassen.

Serveradministration

Dieser Abschnitt enthält konzeptionelle Themen, die sich mit der Serveradministration befassen.

In diesem Abschnitt

Übersicht über Sicherheitsstrategien
Beschreibt die unterschiedlichen Zugriffsrechte und Sicherheitsstrategien, die Sie verwenden können.

Verwendung von Passwörtern
Beschreibt, wie Passwörter erstellt und verwendet werden, um den Zugriff auf Serverkonfigurationen zu steuern.

Server-Zeitlimit-Optionen
Beschreibt die Optionen für die Anmeldesequenz, die Inaktivität, für das Wiederherstellen der Verbindung zum Server und das Zeitlimit bei der Anmeldung.

Online-Bereinigung
Bietet Informationen zum Bereinigen gelöschter Daten bei laufendem Server.

Zugriffsrechte gewähren
Dieser Abschnitt enthält konzeptionelle Themen zum Gewähren von Zugriffsrechten.

Speicherorte für die Datenspeicherung
Dieser Abschnitt enthält konzeptionelle Themen, die sich mit dem Speichern von Daten in StarTeam befassen.

Übersicht über Benutzer- und Gruppenkonfigurationen
Konzeptionelle Informationen zur Konfiguration von Benutzern und Gruppen in StarTeam-Server.

LDAP für die Passwortverifizierung
Beschreibt die Passwortverifizierung mit dem LDAP QuickStart Manager-Verzeichnisdienst von Borland.

Richtlinien für die Serverkonfiguration
Beschreibt die Empfehlungen für die Arbeit mit StarTeam-Serverkonfigurationen.

Atomische Eincheckvorgänge
Dieses Thema beschreibt das Verhalten von atomischen Eincheckvorgängen in StarTeam.

Vault Verify zum Verifizieren von Dateirevisionen
Dieses Thema bietet eine Übersicht über das für Native-II-Datenspeicher verwendete Vault Verify-Dienstprogramm.

Daten von Auscheckvorgängen mit dem Checkout Trace-Dienstprogramm untersuchen
In diesem Thema wird der Zweck des Checkout Trace-Dienstprogramms beschrieben.

Sicherheitsprotokolle
Beschreibt die drei Typen der Sicherheitsprotokolldateien, die von StarTeam zur Aktivitätsverfolgung und Fehlerbehebung generiert werden.

Übersicht über Initialisierungsdateien
Beschreibt den Zweck der unterschiedlichen Initialisierungsdateien.

Testserver verwenden
Beschreibt die Vorteile beim Verwenden eines Testservers.

Backups
Dieser Abschnitt enthält konzeptionelle Themen, die sich mit dem Erstellen von Backups befassen.

Anpassung
Dieser Abschnitt enthält konzeptionelle Themen, die sich mit der Anpassung befassen.

E-Mail-Unterstützung und angepasste E-Mail-Benachrichtigungen
Konzeptionelle Informationen zu angepassten E-Mail-Benachrichtigungen und zur E-Mail-Unterstützung.

Übersicht über Sicherheitsstrategien

Standardmäßig haben alle Benutzer anfänglich Zugriff auf alle Funktionen des Clients. Um unbeabsichtigte Löschvorgänge und andere Probleme zu vermeiden, müssen Administratoren deshalb so früh wie möglich Zugriffsrechte festlegen.

In den folgenden Abschnitten werden Zugriffsrechte beschrieben und allgemeine Sicherheitsrichtlinien zur Verfügung gestellt:

- Allgemeine Sicherheitsrichtlinien.
- Zugriffsrechte auf Serverebene.
- Zugriffsrechte auf Projekt-, Ansichts-, Ordner- und Elementebene.
- Zugriffsrechte auf Komponenten-, Filter- und Abfragenebene.
- Zugriffsrechte für Heraufstufungsstatuswerte.

Allgemeine Sicherheitsrichtlinien

Solange Sie sich noch nicht gut mit Zugriffsrechten auskennen, empfiehlt Borland, dass Sie die im Folgenden beschriebenen Richtlinien befolgen.

Auf dem StarTeam-Server

Sie können auf dem Server über das Dialogfeld "Benutzer-Manager" Benutzer und Gruppen für eine Serverkonfiguration erstellen, während diese ausgeführt wird. Beachten Sie folgende Richtlinien:

- Ändern Sie nicht die Berechtigungen für die Gruppen "All Users", "Administrators", "System Managers" und "Security Administrators".
- Erstellen Sie in der Gruppe "Administratoren" keine zusätzlichen Gruppen.
- Erstellen Sie die benötigten Gruppen als Untergruppen der Gruppe "All Users" oder untereinander. Beispielsweise könnten Sie die folgenden Gruppen erstellen: "Developers", "Testers" und "Others".
- Erstellen Sie Benutzer und weisen Sie diese Gruppen zu. Stellen Sie sicher, dass mindestens zwei Benutzer über Administratorrechte verfügen, falls ein Administrator einmal ausgesperrt sein sollte.

Auf dem Client

Beachten Sie folgende Richtlinien:

- Obwohl Sie sowohl Rechte verweigern als auch gewähren können, empfiehlt es sich, nur Rechte zu gewähren.
- Wenn Sie dennoch Rechte verweigern, sollten Sie die folgenden zwei Regeln beachten: a) Im Dialogfeld "Zugriffsrechte" sollte ein Knoten niemals ausschließlich über Datensätze zu verweigerten Rechten verfügen und b) Stellen Sie sicher, dass die Datensätze eines Knotens mit verweigerten Rechten immer Vorrang vor den Datensätzen mit gewährten Rechten haben.
- Wenn Sie Zugriffsrechte für einen Knoten festlegen, müssen Sie beachten, dass Benutzern, die keine Zugriffsrechte für den Knoten haben (als einzelne Benutzer oder Mitglieder von Gruppen), alle Zugriffsrechte für diesen Knoten auf der jeweiligen Ebene verweigert werden (es sei denn, dass der Benutzer über vorrangige Berechtigungen verfügt).
- Legen Sie zunächst die Zugriffsrechte auf Projektebene fest. Diese Rechte sollten für alle Gruppen (mit Ausnahme der Gruppe "All Users") für jeden Knoten festgelegt werden. Die Knoten sind "Projekt", "Ansicht", "Untergeordnete Ordner", "Datei", Änderungsanforderung", "Anforderung", "Task" und "Thema". Abhängig von der in Ihrem Unternehmen verwendeten Client-Version werden möglicherweise nicht alle Knoten angezeigt.

Die wichtigsten Knoten, für die Rechte auf dieser Ebene festgelegt werden müssen, sind "Projekt" und "Ansicht". Nur im Projektknoten können Zugriffsrechte für das Projekt festgelegt werden. Über den Ansichtsknoten wird der Zugriff auf alle Ansichten auf Ansichtsebene gesteuert. Neu erstellte Ansichten verfügen zunächst lediglich über die hier für alle Ansichten festgelegten Zugriffsrechte. Sie verfügen anfänglich nicht über Zugriffsrechte auf Ansichtsebene.

- Legen Sie anschließend die Zugriffsrechte auf Ansichtsebene fest. Legen Sie Rechte für alle Benutzer und/ oder Gruppen fest, die auf dieser Ebene Zugriff auf alle Knoten benötigen. (Die Knoten sind "Ansicht", "Untergeordnete Ordner", "Datei", Änderungsanforderung", "Anforderung", "Task" und "Thema".)
- Legen Sie nur dann Zugriffsrechte auf Ordnerebene fest, wenn Sie unbedingt Zugriffsrechte für Ordner benötigen. Beachten Sie, dass Ordner diese Einstellungen beibehalten, wenn sie verschoben oder gemeinsam genutzt bzw. wenn sie Teil einer neuen Ansicht werden (so lange, bis der Ordner in der neuen Ansicht verzweigt wird). Beachten Sie weiterhin, dass sich Ordner nur verzweigen, wenn ihre Eigenschaften geändert werden, was nicht sehr häufig geschieht.
- Vermeiden Sie es, Zugriffsrechte für Stammordner zu vergeben, da diese Rechte zu Konflikten mit Rechten auf der Projekt- oder Ansichtsebene führen können.
- Vergeben Sie keine Rechte für Elemente. Beachten Sie, dass Elemente diese Einstellungen beibehalten, wenn sie verschoben oder gemeinsam genutzt bzw. wenn sie Teil einer neuen Ansicht werden (so lange, bis das Element in der neuen Ansicht verzweigt wird).

Zugriffsrechte auf Serverebene

Durch Zugriffsrechte auf Serverebene werden Benutzer autorisiert, Serveradministrationsoperationen auszuführen, z. B. das Ändern von Serverkonfigurationen und das Anzeigen von Protokollen. Zugriffsrechte auf Serverebene umfassen darüber hinaus Rechte zum Erstellen von Projekten und benutzerdefinierten Feldern, das Steuern der Zugriffsrechte auf Komponentenebene und Rechte zum Ausführen bestimmter Operationen und des Notification Agent.

Durch die Zugriffsrechte auf Serverebene werden Benutzer und Gruppen autorisiert, Operationen in einer bestimmten Serverkonfiguration auszuführen. Eine der Optionen legt fest, wer Projekte erstellen darf, wenn die Serverkonfiguration ausgeführt wird, und wer nicht.

Hinweis: Zugriffsrechte auf Serverebene können nur bei aktiviertem Server zugewiesen werden.

Standardmäßig werden der Gruppe "Administrators" alle Projekt- und Serverrechte zugewiesen. Die Gruppe "All Users" verfügt standardmäßig über die Rechte zum Erstellen von Projekten und zum Anzeigen der Serverkonfiguration und des Serverprotokolls.

Zugriffsrechte auf Projekt-, Ansichts-, Ordner- und Elementebene

Anfänglich kann jeder Benutzer, der ein Projekt, eine Ansicht, einen Ordner oder ein Element anzeigen kann, die Zugriffsrechte für diese festlegen. Zugriffsrechte auf Projekt-, Ansichts-, Ordner- und sogar Elementebene sind hierarchisch strukturiert und können durch Gruppenberechtigungen beeinflusst werden.

Wenn Benutzer sich bei einer Serverkonfiguration anmelden, werden sie über ihre Benutzernamen und als Mitglieder der Gruppen, denen sie angehören, identifiziert. Diese Informationen werden als Zugriffs-Token für jeden Benutzer gespeichert. Wenn Benutzer Operationen an Objekten (Projekten, Ansichten, Ordnern und Elementen) ausführen, überprüft der Client diese Token und die Zugriffsrechte für die Objekte, an denen die Benutzer die Operationen ausführen.

Objektzugriffsrechte und Token festlegen

Der StarTeam-Server überprüft Zugriffsrechte auf verschiedenen Ebenen. Zuerst werden die Zugriffsrechte auf ein Objekt im Register **Systemrichtlinie** überprüft, das Sie öffnen können, indem Sie im Serveradministrations-Tool **Tools** ▸ **Konten** ▸ **Systemrichtlinie** wählen.

Wenn Gruppenberechtigungen nicht ignoriert werden, überschreiben sie alle an anderen Orten erstellten Zugriffsrechte und sind diesen übergeordnet. Berechtigungen sind Gruppeneigenschaften, die im Register **Berechtigungen** des Dialogfelds **Gruppeneigenschaften** festgelegt werden.

Ein Benutzer erhält genau die Berechtigungen, die der Gruppe zugewiesen sind, der er angehört. Wenn der Benutzer zwei Gruppen angehört und einer Gruppe Berechtigungen zugewiesen werden, die der anderen nicht zugewiesen sind, erhält der Benutzer diese Berechtigungen trotzdem, da mindestens eine der Gruppen, der er angehört, über diese Berechtigungen verfügt.

Nachdem der Client die Gruppenberechtigungen überprüft hat, werden die Zugriffsrechte für einzelne Objekte geprüft. Die Einstellungen in den Dialogfeldern **Zugriffsrechte** für Projekte, Ansichten, Ordner und einzelne Elemente gewähren oder verweigern Benutzern oder Gruppen das Ausführen von Operationen auf genau diesen Ebenen.

Hinweis: Wenn Sie im Dialogfeld **Zugriffsrechte** Benutzern Rechte auf einer bestimmten Ebene gewähren, werden den hiervon ausgenommenen Benutzern die Rechte auf der gewählten Ebene effektiv verweigert. Es sei noch darauf hingewiesen, dass ein Benutzer, der ein Objekt anzeigen kann und nicht durch bestimmte Zugriffskriterien ("deny records") am Ausführen einer Operation gehindert wird, alle Aktionen ausführen kann, die ihn über einen Datensatz mit gewährten Rechten ("grant record") zugewiesen werden. Dabei spielt es keine Rolle, ob es sich um einen Einzelbenutzer oder ein Mitglied einer Gruppe handelt. Die einzige Ausnahme hiervon tritt in Zusammenhang mit Berechtigungen auf.

Im Folgenden wird zusammenfassend aufgeführt, welche Prüfungen in der beschriebenen Reihenfolge ausgeführt werden, um zu bestimmen, ob ein Benutzer eine Operation ausführen darf:

1. Wenn der Benutzer einer Gruppe mit ausreichenden Berechtigungen angehört und diese nicht ignoriert werden, wird der Zugriff gewährt. Beachten Sie, dass Berechtigungen, wenn sie nicht ignoriert werden, eventuell vorhandenen Zugriffsrechten übergeordnet sind. Benutzer, die einer Gruppe mit den erforderlichen Berechtigungen angehören, erhalten so möglicherweise Zugriffsrechte, die ihnen im Client ausdrücklich verweigert werden.
2. Wenn der Benutzer oder eine Gruppe, der der Benutzer angehört, über die erforderlichen Zugriffsrechte für ein Objekt besitzt, wird dem Benutzer der Zugriff gewährt und er kann die Operation ausführen. Wenn für das Objekt Zugriffsrechte festgelegt wurden, von denen keines ausreichend ist, wird dem Benutzer der Zugriff verweigert.
3. Wenn für das Objekt keine Zugriffsrechte festgelegt wurden, wird die nächst höhere Ebene geprüft. Wenn beispielsweise eine Operation an einer Datei, einer Änderungsanforderung, einem Thema, Task oder Unterordner durchgeführt werden soll, werden die Zugriffsrechte für den übergeordneten Ordner geprüft. Wenn sich die Operation auf einen Stammordner bezieht, werden die Zugriffsrechte für die Ansicht überprüft. Wenn sich die Operation auf eine Ansicht bezieht, werden die Zugriffsrechte für das Projekt überprüft. Wenn sich die auszuführende Operation auf das Erstellen eines Projekts bezieht, werden die Zugriffsrechte für den Server überprüft.
4. Wenn für keine dieser Ebenen Zugriffsrechte festgelegt wurden, wird der Zugriff gewährt.

Als Administrator können Sie Gruppenberechtigungen außer Kraft setzen, indem Sie im Dialogfeld **Systemrichtlinie** der Serverkonfiguration entsprechende Optionen festlegen. Verwenden Sie diese Option mit Vorsicht, da hierdurch die Vorgehensweise des StarTeam-Servers beim Prüfen der Zugriffsrechte aller Benutzer (einschließlich der Administratoren) auf alle Objekte des Repositorys geändert wird. Wenn Berechtigungen nicht berücksichtigt werden, wird ausschließlich durch Zugriffsrechte festgelegt, wer Operationen an Objekten im Repository durchführen darf und wer nicht.

Gruppenberechtigungen für Objekte

Durch die einer Gruppe zugewiesenen Berechtigungen erhalten Mitglieder der Gruppe möglicherweise das Recht, auf Objekte zuzugreifen und Operationen auszuführen, für die sie normalerweise keine Rechte haben. Mit anderen Worten: Gruppenberechtigungen haben Vorrang vor Einstellungen für Zugriffsrechte.

Wenn Sie im Serveradministrations-Tool **Tools** ▸ **Konten** ▸ **Benutzer-Manager** wählen, werden Sie feststellen, dass die Serverkonfiguration über einige Standardgruppen verfügt: "All Users", "Administrators", "System Managers" und "Security Administrators". Der Standardbenutzer mit dem Namen "Administrator" ist Mitglied der Gruppen "Administrators" und "Security Administrators". Standardmäßig verfügt die Administratorengruppe über alle Gruppenberechtigungen. Alle anderen Gruppen verfügen standardmäßig über keine dieser Berechtigungen.

Alle Mitglieder einer Gruppe haben für jedes von der Serverkonfiguration verwaltete Projekt dieselben Berechtigungen. Die Berechtigungen gelten in gleichem Maß für alle Ebenen: Projekte, Ansichten, Ordner und Elemente in Ordnern. Wenn Benutzer mehreren Gruppen angehören, verfügen sie über die maximale Anzahl an Berechtigungen, unabhängig davon, welche Gruppe diese Berechtigungen gewährt.

Objektzugriffsrecht-Ebenen

Zugriffsrechte werden für einzelne Benutzer oder Gruppen auf den folgenden Ebenen festgelegt:

- **Projektebene** Zugriffsrechte können projektweit festgelegt werden. Sie können außerdem Zugriffsrechte festlegen, die für alle Ansichten, Unterordner und Elemente des Projekts gelten, wenn für das jeweilige Objekt nicht eigene Zugriffsrechte festgelegt sind. Auf dieser und anderen Ebenen stehen Ihnen die Knoten "Ansicht", "Untergeordnete Ordner" und weitere Knoten zur Verfügung.
- **Ansichtsebene** Sie können Zugriffsrechte für eine Ansicht festgelegen. Sie können außerdem Zugriffsrechte vergeben, die für alle Unterordner und Elemente gelten, wenn für das jeweilige Objekt nicht eigene Zugriffsrechte festgelegt sind.
- **Ordnerebene** Sie können Zugriffsrechte für einen Ordner festlegen. Sie können außerdem Zugriffsrechte vergeben, die für alle Unterordner und Elemente gelten, wenn für das jeweilige Objekt nicht eigene Zugriffsrechte festgelegt sind.
- **Elementebene** Sie können Zugriffsrechte für eine bestimmte Datei, eine Änderungsanforderung, eine Anforderung, einen Task oder ein Thema festlegen. (Es ist ungewöhnlich, auf dieser Ebene Rechte festzulegen.)

Beachten Sie, das Zugriffsrechte für das Projekt nur auf der Projektebene vergeben werden können, da es nur auf dieser Ebene in der Hierarchie der Zugriffsrechte den Knoten "Projekt" gibt. Zugriffsrechte für Ansichten können entweder auf Projekt- oder Ansichtsebene festgelegt werden, da es auf beiden Ebenen den Knoten "Ansicht" gibt. Zugriffsrechte für Ordner können entweder auf Projekt-, Ansichts- oder Ordnerebene festgelegt werden usw.

Projekte und Ansichten öffnen

Ein Projekt kann von seiner Stammansicht und vom Stammordner dieser Ansicht nicht unterschieden werden. Tatsächlich können alle Ansichten eines Projekts nicht von ihrem Stammordner unterschieden werden. Daher kann ein Benutzer ein Projekt nicht öffnen, wenn Sie dem Benutzer (oder allen Gruppen, denen der Benutzer angehört) eines der folgenden Rechte verweigern:

- Das Recht, das Projekt anzuzeigen.
- Das Recht, die Stammansicht des Projekts anzuzeigen.
- Das Recht, den Stammordner der Anfangsansicht des Projekts anzuzeigen.

Ein Benutzer kann eine bestimmte Projektansicht nicht öffnen, wenn ihm (oder allen Gruppen, denen er angehört) eines der folgenden Rechte verweigert wird:

- Das Recht, die Ansicht anzuzeigen.

- Das Recht, den Stammordner der Ansicht anzuzeigen.

Zugriffsrechte auf Komponenten-, Filter- und Abfrageebene

Die Client-Komponenten ("Datei", "Änderungsanforderung", "Anforderung", "Task" und "Thema") sind Serverobjekte. Die Komponente "Änderungsanforderung" wird beispielsweise in jeder Projektansicht angezeigt und verfügt in allen Ansichten über dieselben Filter und Abfragen.

Zugriffsrechte auf Komponentenebene regeln die Verwendung von Filtern und Abfragen für jede Komponente. Sie legen fest, welche Benutzer öffentliche Filter und Abfragen für diese Komponente erstellen können, wer die Filter und Abfragen verwenden kann usw. Mit dem Zugriffsrecht auf Serverebene namens **Zugriffsrechte für Komponenten verwalten** können Benutzer diese Rechte festlegen.

Einzelne Filter und Abfragen verfügen ebenfalls über Zugriffsrechte. Diese Rechte haben Vorrang vor den allgemeinen Zugriffsrechten für Filter und Abfragen.

Das rechte Teilfenster enthält eine Baumstruktur der Unterkategorien der Zugriffsrechte. Wird diese Struktur erweitert, zeigt jede Unterkategorie die entsprechenden Zugriffsrechte als untergeordnete Objekte an.

Filter und Abfragen befinden sich in bestimmten Komponenten (z. B. Komponente "Änderungsanforderung" oder "Datei"). Sie können ausschließlich auf die Daten der jeweiligen Komponente in allen Projektansichten angewendet werden, die von einer bestimmten Serverkonfiguration verwaltet werden.

Alle Benutzer können private Filter und Abfragen erstellen, aber für öffentliche Filter und Abfragen gibt es einzelne und komponentenspezifische Zugriffsrechte. Für einzelne Filter oder Abfragen festgelegte Zugriffsrechte haben Priorität vor Zugriffsrechten auf Komponentenebene.

Um einen öffentlichen Filter oder eine Abfrage anzuwenden, muss ein Benutzer das Recht haben, in einer geöffneten Projektansicht auf den Datentyp der jeweiligen Komponente zuzugreifen. Wenn Sie Filter oder Abfragen anwenden, betrifft dies die sichtbaren Daten des gewählten Typs in der Projektansicht.

Benutzer können alle öffentlichen Filter und Abfragen anwenden, die sie anzeigen können. Im Allgemeinen werden Benutzern die öffentlichen Filter und Abfragen angezeigt, für die sie über die erforderlichen Zugriffsrechte verfügen.

Zugriffsrechte für Heraufstufungsstatuswerte.

Jede Ansicht verfügt über einen eigenen Satz von Heraufstufungsstatuswerten. Der Zugriff auf diese Statuswerte wird durch Folgendes gesteuert:

- Das Recht "Heraufstufungsmodell festlegen".
- Zugriffsrechte, die den Zugriff auf einzelne Heraufstufungsstatuswerte steuern.

Das Recht 'Heraufstufungsmodell festlegen'.

Das Recht **Heraufstufungsmodell festlegen** kann im **Ansichtsknoten** des Dialogfelds **Zugriffsrechte** auf Ansichts- und Projektebene festgelegt werden. Benutzer mit dem Recht zum Festlegen eines Heraufstufungsmodells können folgende Aktionen für das Heraufstufungsmodell ausführen:

- Statuswerte erstellen und löschen.
- Eigenschaften von Statuswerten bearbeiten.
- Ein Label auf einen anderen Status heraufstufen. Die Heraufstufung ist der Bearbeitung von Eigenschaften untergeordnet. Benutzer mit dem Recht zum Bearbeiten der Eigenschaften können einen Status auch heraufstufen.

- Statuswerte in einer Ansicht neu anordnen.

Zugriffsrechte für Heraufstufungsstatuswerte

Heraufstufungsstatusrechte steuern den Zugriff auf einzelne Heraufstufungsstatuswerte. Diese allgemeinen Rechte für Objekte und spezifischen Rechte für Heraufstufungsstatuswerte können im Knoten "Heraufstufungsstatus" des Dialogfelds "Zugriffsrechte" auf Ansichts- und Projektebene festgelegt werden. Sie werden außerdem bei den Zugriffsrechten für einzelne Heraufstufungsstatuswerte angezeigt.

Die Rechte für einen einzelnen Heraufstufungsstatus werden auf der Statusebene und, falls nötig, weiter auf der Ansichtsebene und eventuell auf der Projektebene geprüft. Wenn einem Benutzer ein bestimmtes Zugriffsrecht auf einer Ebene gewährt wird, muss die folgende Ebene nicht geprüft werden.

Wird ein Zugriffsrecht auf Ansichtsebene gewährt, gilt es für alle Statuswerte der Ansicht, sofern der Zugriff auf Statusebene nicht verweigert wird.

Wird ein Zugriffsrecht auf Projektebene gewährt, gilt es für alle Statuswerte in allen Ansichten des Projekts, sofern der Zugriff auf Status- oder Ansichtsebene nicht verweigert wird.

Verwandte Konzepte

Zugriffsrechte gewähren

Verwandte Referenz

Zugriffsrechte und Berechtigungen

Verwendung von Passwörtern

Passwörter sind für den Serveradministrator und für Benutzer für den Zugriff auf StarTeam-Serverkonfigurationen erforderlich. Beim Erstellen der Serverkonfiguration wird standardmäßig ein Serveradministratorkonto mit dem Benutzernamen und dem Kennwort "Administrator" erstellt. Dieses Passwort sollte sofort geändert werden. Wenn der Serveradministrator einen Benutzer hinzufügt, wird ein eindeutiger Benutzername und ein Passwort gemäß den für diese Serverkonfiguration angegebenen Passworteigenschaften erstellt.

Der Serveradministrator legt die Passworteigenschaften für jede Serverkonfiguration im Dialogfeld **Tools ▸ Konten ▸ Systemrichtlinie** im Register **Passwörter** fest. Die festgelegte Systemrichtlinie für Passwörter gilt für alle Benutzer, die auf diese Serverkonfiguration zugreifen.

Zu den Passworteigenschaften gehören die Gültigkeitsdauer für Passwörter, die minimale Länge und die Verwendung sicherer Passwörter.

Allgemeines zu sicheren Passwörtern

Der Serveradministrator kann festlegen, dass für Benutzer, die auf eine Serverkonfiguration zugreifen, ein sicheres Passwort erforderlich ist. Wenn die Systemrichtlinie für diese Serverkonfiguration ein sicheres Passwort erfordert, muss dieses folgende Bedingungen erfüllen:

- Es muss eindeutig sein und darf nicht wiederholt verwendet werden.
- Es muss sich vom Benutzernamen unterscheiden.
- Es muss mindestens einen Klein- und einen Großbuchstaben enthalten. (Maßgeblich hierfür ist das Basisalphabet mit 26 Buchstaben.)
- Es muss mindestens ein nicht alphabetisches Zeichen enthalten.

Standardmäßig ist die Option für die Verwendung von sicheren Passwörtern deaktiviert.

Änderungen der Passworteigenschaften

Wenn der Systemadministrator die Passworteigenschaften für eine Serverkonfiguration ändert, ist der Zeitpunkt, ab dem die Änderungen wirksam werden, abhängig von der Eigenschaft.

Änderungen, die an der Passwortlänge vorgenommen werden, sind sofort wirksam, gelten aber nur für alle neuen Benutzerkonten oder neue Passwörter. Wenn Sie beispielsweise die Mindestlänge für Passwörter von acht in zehn Zeichen ändern, müssen alle neuen Benutzer Passwörter verwenden, die mindestens zehn Zeichen lang sind. Bereits vorhandene Benutzer können jedoch weiterhin ihre acht Zeichen langen Passwörter verwenden.

Änderungen, die an der Gültigkeitsdauer für Passwörter vorgenommen wurden, werden nach dem entsprechenden Zeitintervall wirksam. Wenn Sie beispielsweise die Gültigkeitsdauer für Passwörter auf dreißig Tage setzen, werden die Benutzerkonten gesperrt, wenn die entsprechenden Passwörter vor Ablauf des Zeitraums nicht geändert wurden. Benutzer werden zwei Wochen vor der Sperrung aufgefordert, das Passwort zu ändern. Nur das Administratorkonto verliert nie seine Gültigkeit.

Wenn die Option für sichere Passwörter aktiviert ist, wird sie nur auf neue Benutzer und Benutzer angewendet, die ihre Passwörter ändern. Die alten "nicht sicheren" Passwörter bleiben bis zu einer solchen Passwortänderung gültig.

Hinweis: Der Systemadministrator kann eine Passwortänderung erzwingen, wenn Benutzer eine Änderung einer Passworteigenschaft sofort übernehmen sollen oder wenn für ein Projekt ein Sicherheitsverstoß aufgetreten ist.

Verwandte Verfahrensweisen

Benutzerpasswörter ändern
Passwortänderung erzwingen
Passworteinschränkungen konfigurieren

Server-Zeitlimit-Optionen

Sie können folgende Zeitlimit-Optionen für den Server festlegen:

- Zeitlimit beim Anmeldevorgang.
- Inaktivitäts-Zeitlimit.
- Zeitlimit bei der Wiederherstellung der Verbindung.
- Anzahl der Anmeldeversuche.

Zeitlimit beim Server-Anmeldevorgang

Die Einstellung "Zeitlimit beim Anmeldevorgang" gilt für Clients und die Serverkonfiguration. Sie gibt die maximale Zeitdauer an, in der der Client die Verbindung zum Server herstellen muss. Wenn das Zeitlimit überschritten wird und die Verbindung nicht hergestellt wurde, muss der Benutzer erneut versuchen, sich anzumelden.

Mit der Option **Zeitlimit beim Anmeldevorgang** im Dialogfeld **Server konfigurieren** können Sie den Wert für das Zeitlimit beim Anmeldevorgang festlegen. Diese Operation kann nur bei aktiviertem Server ausgeführt werden.

Zeitlimit für Serverinaktivität

Das Zeitlimit für Inaktivität ist eine Sicherheitsfunktion, die beinhaltet, dass Benutzer automatisch abgemeldet werden, wenn sie für den vom Administrator bestimmten Zeitraum inaktiv bleiben. Wenn ein Client während des angegebenen Zeitraums nicht mit der Serverkonfiguration kommuniziert (weder automatisch noch manuell), bricht der Server die Verbindung ab. Wenn keine anderen Serververbindungen mit der Benutzersitzung vorhanden sind, wird die Benutzersitzung vom Server entfernt. Wenn der Benutzer eine Lizenz für gleichzeitige Benutzer hat, wird die Lizenz automatisch an den Pool für Lizenzen für gleichzeitige Benutzer zurückgegeben. Der Benutzer muss sich anschließend erneut anmelden, um die Verbindung wiederherstellen zu können.

Sie können die Option **Zeitlimit für Inaktivität** im Dialogfeld **Server konfigurieren** verwenden, um den Wert für das Zeitlimit für Inaktivität festzulegen. Damit benannte Benutzer (Benutzer mit personengebundener Lizenz) auch dann angemeldet bleiben, wenn sie das Zeitlimit für Inaktivität überschreiten, können Administratoren nach Auswahl der Option **Zeitlimit für Inaktivität** und Angabe eines Zeitlimits die Option **Benannte Benutzer ausschließen** auswählen.

Auch wenn ein Zeitlimit für Inaktivität festgelegt ist, werden Benutzer nicht abgemeldet, wenn in den Optionen für Systembenachrichtigungen ein kürzerer Zeitraum als für das Zeitlimit für Inaktivität ausgewählt wurde. Angenommen, ein Benutzer hat die Benachrichtigungen so konfiguriert, dass die Funktion alle zehn Minuten automatisch auf neue Änderungsanforderungen prüft, und das Zeitlimit für Inaktivität ist auf 60 Minuten eingestellt. In diesem Fall überschreitet der Benutzer aufgrund der automatischen Kommunikation zwischen dem Client und dem Server das Zeitlimit nie.

Zeitlimit für die Wiederherstellung der Verbindung zum Server

Wenn ein Client seine Netzwerkverbindung verliert, wird die Verbindung der Benutzer mit dem Server unterbrochen. Mithilfe der Option "Zeitlimit für Neuverbindung" wird die Zeitspanne festgelegt, während der der Client die Verbindung erneut herstellen muss. Der Client versucht, die Verbindung nur dann wiederherzustellen, wenn der Benutzer versucht, einen Befehl an den Server zu senden. Eine erneut hergestellte Verbindung verfügt über den vollständigen Kontext der verlorenen Verbindung.

Wenn der Client die Verbindung mit dem Server während des eingestellten Zeitlimits erfolgreich wiederherstellt, können Benutzer einfach mit Ihrer Arbeit im Programm fortfahren. Sie müssen nicht ihre Projekte schließen, sich

erneut anmelden und ihre Ansichtseinstellungen wiederherstellen. Wenn jedoch das Zeitlimit für eine Neuverbindung abgelaufen ist, müssen Sie den Client entweder schließen oder sich erneut beim Server anmelden.

Mit der Option **Zeitlimit für Neuverbindung** im Dialogfeld **Server konfigurieren** können Sie den Wert des Zeitlimits für die Neuverbindung festlegen. Das Zeitlimit für Neuverbindung kann nur auf einem aktiven Server geändert werden. Dies ist nicht möglich, wenn der Server neu gestartet wurde.

Hinweis: Wenn der Server neu gestartet werden muss, kann der Client die Verbindung zum Server nicht automatisch wiederherstellen.

Wenn Sie das **Zeitlimit für Inaktivität** festlegen, setzen Sie dieses auf einen höheren Wert als das **Zeitlimit für Neuverbindung**. Anderenfalls wird, wenn sowohl das **Zeitlimit für Neuverbindung** als auch das **Zeitlimit für Inaktivität** aktiviert sind und das **Zeitlimit für Inaktivität** kürzer ist, der Benutzer abgemeldet, bevor der Client die Verbindung wiederherstellen kann. Dies bedeutet, dass, wenn das **Zeitlimit für Neuverbindung** länger als das **Zeitlimit für Inaktivität** ist und beide aktiviert sind, dann tritt das **Zeitlimit für Inaktivität** in Kraft, bevor das **Zeitlimit für Neuverbindung** abgelaufen ist.

Anzahl der Anmeldeversuche.

Sie können die Sicherheit Ihrer Projekte erhöhen, indem Sie Einstellungen für Anmeldefehler und Zeitlimits für Anmeldevorgänge festlegen. Eine Ursache für Anmeldefehler kann sein, dass Hacker versuchen, Benutzerpasswörter auszuspionieren. In solchen Fällen sollten Sie die IP-Adresse des Systems möglicherweise ändern, um es den Angreifern zu erschweren, die Serverkonfiguration zu finden und ihre Angriffe zu wiederholen. Gegebenenfalls sollten Sie auch die Benutzernamen aller Benutzer des Systems ändern.

Wählen Sie **Tools ▸ Konten ▸ Systemrichtlinie**, legen Sie dann im Register **Fehler bei der Anmeldung** fest, wie Fehlschläge bei der Anmeldung gehandhabt werden, und geben Sie die Länge einer Sperre an, sofern diese verwendet wird. Sie können die Serverkonfiguration so konfigurieren, dass Mitglieder der Gruppe "Security Administrators" per E-Mail über fehlgeschlagene Anmeldungen und Kontosperrungen benachrichtigt werden. Diese Operation kann nur bei aktiviertem Server ausgeführt werden.

Jedes Benutzerkonto, auch das eines Administrators, kann für eine Serverkonfiguration gesperrt werden, wenn die Anzahl der Anmeldeversuche mit einem falschen Passwort überschritten wird. Die Sperrzeit für das Hauptverwaltungskonto (Administrator) beträgt 24 Stunden. Sie können das Administratorkonto jedoch vor Ablauf der 24 Stunden entsperren (weitere Informationen hierzu finden Sie unter "Administrative Konten reaktivieren" unter "Verwandte Informationen".)

Verwandte Verfahrensweisen

Server-Zeitlimit-Optionen ändern
Anzahl der möglichen Anmeldeversuche konfigurieren
Administrative Konten reaktivieren
E-Mail-Unterstützung und angepasste E-Mail-Benachrichtigungen

Online-Bereinigung

Bei der Online-Bereinigung werden gelöschte Daten bei laufendem Server bereinigt. Der Bereinigungsvorgang löscht unerwünschte Daten aus der Datenbank und entfernt gelöschte Archive aus dem Datenspeicher. In den Vorgängerversionen musste immer der Server heruntergefahren werden, bevor eine Bereinigung durchgeführt werden konnte.

Die Online-Bereinigung bei laufendem Server verhindert die teuren Ausfallzeiten einer Offline-Bereinigung, die einige Stunden bis einige Tage dauern konnten. Die Online-Bereinigung macht diese kostspieligen Ausfallzeiten nicht nur überflüssig, sie ist auch noch wesentlich schneller als eine Offline-Bereinigung.

Der Prozess der Online-Bereinigung kann auf dem Register für die Online-Bereinigung im Serveradministrations-Tool gestartet und gestoppt werden. Sie können die Online-Bereinigung sowohl auf einem Remote-Server als auch auf einem lokalen Server starten und stoppen.

Neu gelöschte Daten stehen bei der Online-Bereinigung nur dann zum Bereinigen zur Verfügung, nachdem ein Neustart des Servers durchgeführt wurde. Die Online-Bereinigung ist ein interaktiver Prozess, der jederzeit gestartet und gestoppt werden kann, solange der Server läuft. Die Online-Bereinigung zeichnet ihren aktuellen Ausführungsstatus auf und kann exakt von dem Punkt aus neu gestartet werden, an dem sie gestoppt wurde. Nach einem Neustart des Servers muss die Online-Bereinigung manuell neu gestartet werden.

Hinweis: Die Offline-Bereinigung ist in StarTeam 2009 weiterhin verfügbar, wird aber in nachfolgenden Versionen entfernt.

Zugriffsrechte gewähren

Wannn und wie Sie Zugriffsrechte gewähren, hängt von vielen Punkten ab.

In diesem Abschnitt

Zugriffsrechte auf Projektebene gewähren
Beschreibt die Regeln für das Gewähren von Zugriffsrechten auf Projektebene.

Zugriffsrechte auf Ansichtsebene gewähren
Beschreibt die Regeln für das Gewähren von Zugriffsrechten auf Ansichtsebene.

Zugriffsrechte auf Ordnerebene gewähren
Beschreibt die Regeln für das Gewähren von Zugriffsrechten auf Ordnerebene.

Zugriffsrechte auf Elementebene gewähren
Beschreibt die Regeln für das Gewähren von Zugriffsrechten auf Elementebene.

Zugriffsrechte verweigern
Beschreibt die Regeln für das Verweigern von Zugriffsrechten für Objekte.

Allgemeine Regeln für Zugriffsrechte
Beschreibt die allgemeinen Regeln für das Gewähren von Zugriffsrechten für Objekte.

Zugriffsrechte und Gruppenberechtigungen
Beschreibt, wie Gruppenberechtigungen und Zugriffsrechte zusammenhängen.

StarTeam SDK-Verbindungssteuerung
Beschreibt, wie verhindert werden kann, dass unerwünschte SDK-Anwendungen eine Verbindung zum Server herstellen und Serverressourcen binden.

Zugriffsrechte auf Projektebene gewähren

Dieser Abschnitt enthält Informationen über das Festlegen von Zugriffsrechten auf Projektebene. Diese Informationen werden durch ein Beispiel mit drei benutzerdefinierten Gruppen verdeutlicht: **Developers**, **Testers**, und **Others**. (Diese Gruppen wurden zu den mit dem StarTeam-Server ausgelieferten Standardgruppen **All Users**, **Administrators**, **System Managers** und **Security Administrators** hinzugefügt.) In dem Beispiel wird davon ausgegangen, dass die Gruppe **All Users** größer ist als die Gruppe **Others**.

Der Knoten 'Projekt'

Angenommen, Sie entscheiden, dass nur Mitglieder der Gruppe **Administrators** das Projekt steuern sollen, und gewähren die entsprechenden Rechte. Durch diese Einstellung können nur Mitglieder der Gruppe **Administrators** das Projekt anzeigen, wenn keine vorrangigen Berechtigungen vorliegen. Somit kann niemand anderes auf die Objekte des Projekts zugreifen und mit diesen arbeiten.

Hinweis: Obwohl die Mitglieder der Gruppe **Administrators** alle Zugriffsrechte für das Projekt benötigen, können Sie diese aus der Liste "Benutzer- und Gruppen" entfernen, wenn sie über Gruppenberechtigungen verfügen. Dies ist normalerweise möglich. Wenn die Serverkonfiguration jedoch so konfiguriert ist, dass Berechtigungen ignoriert werden, müssen Sie der Gruppe **Administrators** alle Zugriffsrechte auf Projektebene speziell zuweisen.

Als Nächstes müssen Sie allen anderen Gruppen, die auf das Projekt zugreifen müssen, die benötigten Rechte zuweisen. Da die Schlüsselworterweiterung eine Projekteigenschaft ist, benötigt die Gruppe **Developers** Rechte zum Anzeigen des Projekts und zum Ändern der Projekteigenschaften. Wahrscheinlich müssen sie das Projekt jedoch nicht löschen oder die Zugriffsrechte ändern. Die Gruppen **Testers** und **Others** müssen das Projekt und seine Eigenschaften anzeigen, daher sollten Sie nur das Auswahlfeld **Objekt und seine Eigenschaften anzeigen** für diese Gruppen aktivieren.

Der Knoten 'Ansicht'

Auf Projektebene festgelegte Zugriffsrechte für Ansichten gelten für alle Ansichten, die bereits vorhanden sind oder zukünftig für das Projekt erstellt werden. Die Mitglieder der Gruppe **Administrators** benötigen alle Rechte für Ansichten. Sie können diese Rechte zugewiesen bekommen oder aufgrund ihrer Berechtigungen erhalten. Die Gruppen **Developers** und **Testers** benötigen Rechte zum Anzeigen und Ändern der Ansichtseigenschaften und zum Ausführen von Operationen mit Labels. Sie benötigen keine Rechte zum Erstellen oder Löschen von Ansichten, zum Verwalten von Heraufstufungsstatuswerten oder zum Ändern der Zugriffsrechte für Ansichten. Die Gruppe **Others** benötigt ausschließlich das Recht zum Anzeigen der Ansicht:

Der Knoten 'Heraufstufungsstatus'

Der Knoten "Heraufstufungsstatus" spielt in diesem Beispiel keine Rolle.

Der Knoten 'Untergeordnete Ordner'

Die Gruppe **Administrators** benötigt möglicherweise sämtliche Zugriffsrechte für untergeordnete Ordner auf Projektebene. Sie können diese Rechte zugewiesen bekommen oder aufgrund ihrer Berechtigungen erhalten. Die Gruppen **Developers** und **Testers** benötigen vermutlich keine Rechte zum Löschen, Freigeben oder Verschieben von Ordnern, zum Ändern des Ordnerverhaltens bzw. der Ordnerkonfigurationen oder zum Ändern der Zugriffsrechte für Ordner. Möglicherweise möchten Sie festlegen, dass die Gruppe **Others** nur das Recht zum Anzeigen der Ordner, ihrer Eigenschaften und ihrer Historien erhält.

Die Elementknoten

Borland empfiehlt, dass Sie mehr als einen Datensatz zur Gewährung bzw. Verweigerung von Rechten für einen einzelnen Knoten anlegen. Im folgenden Abschnitt wird exemplarisch für Dateien beschrieben, wie auf Projektebene Zugriffsrechte für Elemente zugewiesen werden können.

Wenn nur die Entwickler auf Dateien zugreifen müssen, können Sie die Zugriffsrechte für Dateien auf Projektebene auf die Gruppe **Developers** beschränken.

Mit dieser Einstellung verfügen ausschließlich die Mitglieder der Gruppe **Developers** unabhängig von der Ansicht, dem Ordner oder der Datei über Zugriffsrechte auf alle Dateien. Somit können nur Entwickler Dateien anzeigen oder Operationen mit diesen ausführen. Die Mitglieder der Gruppen **Testers** und **Others** können nur die Dateien anzeigen, die sich in ihren Arbeitsordnern befinden, aber der Status dieser Dateien wird als **Nicht in Ansicht** angezeigt. Standardmäßig gibt es jedoch eine Ausnahme durch das Verwenden von **Berechtigungen**. Wenn andere Gruppen als die **Entwickler** über mindestens eine Berechtigung verfügen, die es ihnen erlaubt, eine Datei anzuzeigen, zu ändern, zu definieren oder andere Aktionen mit der Datei auszuführen, erhalten die Mitglieder dieser Gruppen unabhängig von den festgelegten Zugriffsrechten Zugriff auf diese Dateien. Die Standardeinstellungen der Gruppe **Administrators** gewähren der Gruppe alle Berechtigungen. Daher können Mitglieder dieser Gruppe alle Dateioperationen ausführen.

Sie können verhindern, dass die Serverkonfiguration auf Berechtigungen prüft.

Wenn Sie nur den Gruppen **Testers** und **Developers** Zugriff auf andere Elementtypen (Änderungsanforderungen, Anforderungen, Tasks und Themen) gewähren, gelten dieselben Ausnahmen. Es werden jedoch weitere Gruppen Zugriffsrechte für diese Elementtypen benötigen, daher müssen Sie diesen Gruppen einige Zugriffsrechte gewähren.

Verwandte Konzepte

Übersicht über Sicherheitsstrategien
Zugriffsrechte gewähren

Verwandte Verfahrensweisen

Zugriffsrechte und Gruppenberechtigungen verwalten

Zugriffsrechte auf Ansichtsebene gewähren

Üblicherweise können Zugriffsrechte auf Projektebene nicht genau genug festgelegt werden. Beispielsweise kann es vorkommen, dass eine Entwicklergruppe Release 1.0 eines Produkts als eine Ansicht anzeigt, während eine zweite Entwicklergruppe in einer anderen Ansicht am Quellcode für Release 2.0 arbeitet.

In dieser Situation sollten Sie neue Gruppen erstellen, beispielsweise "Entwickler von 1.0", "Entwickler von 2.0", "Tester von 1.0" und "Tester von 2.0". Sie können den Entwicklern und Testern von 1.0 Zugriff auf Dateien und/oder Änderungsanforderungen in der Ansicht "Release 1.0" gewähren und anschließend den Entwicklern und Testern von 2.0 Zugriff auf Dateien und/oder Änderungsanforderungen der Ansicht "Release 2.0" gewähren.

Hierzu müssen Sie Zugriffsrechte auf Ansichtsebene festlegen. Sie müssen jedoch weiterhin Zugriffsrechte für das Projekt auf Projektebene festlegen, da nur auf dieser Ebene der Projektknoten angezeigt wird.

Zugriffsrechte für Ansichten und untergeordnete Ansichten

Auf Ansichtsebene festgelegte Zugriffsrechte für eine untergeordnete Ansicht sind unabhängig von den auf Ansichtsebene festgelegten Zugriffsrechten für die übergeordnete Ansicht. Daher verfügt eine untergeordnete Ansicht zunächst über keine Zugriffsrechte auf Ansichtsebene.

Neue untergeordnete Ansichten werden im Repository durch andere Objekte dargestellt als ihre übergeordneten Ansichten. Sie haben andere Namen, Beschreibungen, Positionen in der Ansichtshierarchie usw.

Zugriffsrechte auf Ansichtsebene können für neue untergeordnete Ansichten festgelegt werden. Angenommen, eine Referenzansicht enthält nur einen Zweig der Ordnerhierarchie der übergeordneten Ansicht. Die Referenzansicht hat einen Stammordner namens "QA Tests". In diesem Fall können Sie in der Referenzansicht ausschließlich den **Testern** Zugriffsrechte für Dateien gewähren, auch wenn in der übergeordneten Ansicht ausschließlich die **Entwicklergruppe** über Zugriffsrechte für Dateien verfügt.

Zugriffsrechte auf unterschiedlichen Ebenen

Manchmal hat eine Gruppe für denselben Objekttyp in derselben Ansicht andere Zugriffsrechte auf der Ansichts- als auf der Projektebene. In diesem Fall werden die Zugriffsrechte auf der niedrigsten Ebene angewendet.

Der StarTeam-Server beginnt bei der Suche nach Zugriffsrechten mit der niedrigsten Ebene und fährt dann mit der nächst höheren Ebene fort. Wenn das Programm eine Ebene findet, auf der einer Gruppe Zugriffsrechte gewährt wurden, setzt es die Suche nach dem jeweiligen Objekttyp nicht auf höheren Ebenen fort.

Beachten Sie, dass Zugriffsrechte für Projekte nur auf Projektebene vorhanden sind, sodass derartige Rechte immer auf Projektebene gesucht werden. Zugriffsrechte für Dateien können jedoch auf Datei-, Ordner-, Ansichts- und Projektebene vorhanden sein. Der Server beendet die Suche bei der ersten Ebene, auf der Zugriffsrechte für Dateien gewährt wurden.

Verwandte Konzepte

Übersicht über Sicherheitsstrategien
Zugriffsrechte gewähren

Verwandte Verfahrensweisen

Zugriffsrechte und Gruppenberechtigungen verwalten

Zugriffsrechte auf Ordnerebene gewähren

Zugriffsrechte auf Ordnerebene werden üblicherweise festgelegt, wenn bestimmte Gruppen (aber keine anderen Gruppen) Zugriff auf einen bestimmten Zweig der Ordnerhierarchie erhalten sollen. Beispielsweise soll nur die Gruppe **Autoren** auf den Zweig mit dem Stammordner "User Manuals" zugreifen.

Das Festlegen von Zugriffsrechten auf Ordner- und auf Elementebene hat weiter reichende Auswirkungen als das Festlegen von Rechten auf höheren Ebenen. Wenn eine untergeordnete Ansicht aus einer übergeordneten Ansicht abgeleitet wird (z. B. alle Referenzansichten und die meisten Verzweigungsansichten), enthält sie im Allgemeinen anfänglich Objekte, die der übergeordneten Ansicht angehören. In Verzweigungsansichten können sich diese Objekte dann zu neuen Objekten verzweigen, die nur in der Unteransicht vorhanden sind. Genau wie für eine neue Ansicht anfänglich keine Zugriffsrechte auf Ansichtsebene festgelegt sind, haben Ordner und Elemente, die in neue Objekte verzweigt werden, anfänglich keine Zugriffsrechte auf Ordner- oder Elementebene.

Die Knoten 'Dieser Ordner' und 'Untergeordnete Ordner'

Auf Ordnerebene gibt es zwei Knoten: den Knoten "Dieser Ordner" für den ausgewählten Ordner und "Untergeordnete Ordner" für die anderen Ordner der Ordnerhierarchie des Zweigs. Mit dieser Funktion können Sie unterschiedliche Zugriffsrechte für jeden Knoten festlegen.

Auf dem Client ist der Stammordner einer Ansicht manchmal schwer von der Ansicht selbst zu unterscheiden. Wenn die Ansicht die Stammansicht (oder anfängliche Ansicht) eines Projekts ist, kann es sein, dass der Stammordner nicht vom Projekt unterscheidbar ist.

Durch das Festlegen von Zugriffsrechten für den Stammordner mithilfe des Knotens **Dieser Ordner** wird möglicherweise der Zugriff eines Benutzers auf die Ansicht beeinflusst. Wenn die Ansicht die Stammansicht ist, wird möglicherweise auch der Zugriff des Benutzers auf das Projekt beeinflusst. Daher vermeiden die meisten Administratoren das Festlegen von Zugriffsrechten auf Ordnerebene, da sich diese Rechte möglicherweise mit anderen Rechten auf Ansichts- oder Projektebene überschneiden.

Angenommen, den Entwicklern wurde das Recht zum Anzeigen des Ordners **User Manuals** nicht zugewiesen und dieser Ordner ist der Stammordner einer Referenzansicht. Die Mitglieder der Gruppe **Entwickler** können die Ansicht nicht öffnen, auch wenn sie auf Ansichtsebene über die notwendigen Zugriffsrechte zum Anzeigen der Ansicht verfügen. Eine Fehlermeldung wird angezeigt, wenn sie versuchen, die Ansicht zu öffnen. Benutzer, die das Recht zum Anzeigen eines Projekts, aber nicht der Stammansicht haben, erhalten ebenfalls eine Fehlermeldung.

Zugriffsrechte für untergeordnete Ansichten

Wenn eine untergeordnete Ansicht Unterordner enthält, für die in der übergeordneten Ansicht Zugriffsrechte festgelegt wurden, erhält die Unteransicht unterschiedliche Zugriffsrechte, je nachdem, ob es sich um eine Referenzansicht oder eine Verzweigungsansicht handelt.

Zugriffsrechte in einer Referenzansicht

Die Zugriffsrechte für eine Referenzansicht auf Ordnerebene sind abhängig von den auf Ordnerebene festgelegten Zugriffsrechten der übergeordneten Ansicht, da keine Verzweigung stattfindet. Wenn Sie über die erforderlichen Rechte verfügen, können Sie die Zugriffsrechte in beiden Ansichten anzeigen.

Wenn Sie in der Referenzansicht Zugriffsrechte ändern, werden diese gleichzeitig auch in der übergeordneten Ansicht geändert (und umgekehrt), da es sich bei dem Ordner in der Referenzansicht um dasselbe Objekt wie den Ordner in der übergeordneten Ansicht handelt.

Zugriffsrechte in einer Verzweigungsansicht

Wenn die untergeordnete Ansicht eine Verzweigungsansicht ist, sind die Zugriffsrechte der untergeordneten Ansicht von den auf Ordnerebene festgelegten Zugriffsrechten der übergeordneten Ansicht unabhängig, nachdem der Ordner in der Verzweigungsansicht tatsächlich verzweigt wurde.

Anfänglich sind alle in der Verzweigungsansicht angezeigten Ordner mit den entsprechenden Objekten der übergeordneten Ansicht identisch. Daher verfügen sie in beiden Ansichten über dieselben Zugriffsrechte. Zunächst können Sie die Zugriffsrechte in der übergeordneten Ansicht ändern (und umgekehrt), da der Ordner in der Verzweigungsansicht dasselbe Objekt ist wie der Ordner in der übergeordneten Ansicht. Nachdem der Ordner verzweigt wurde, wird jedoch ein neues Objekt für den Ordner in der Verzweigungsansicht erstellt. Dieses Objekt beginnt einen eigenen Lebenszyklus und hat im Folgenden keine Zugriffsrechte auf Ordnerebene mehr.

Hinweis: Beachten Sie, dass bei der Verzweigung eines Ordners nicht auch der Inhalt des Ordners verzweigt wird. Jedes Element des Ordners wird einzeln behandelt.

Das Verhalten von Ordnern in einer Verzweigungsansicht wirkt sich auf die Zugriffsrechte aus:

- Wenn ein Ordner bei Änderungen verzweigt wird und Sie eine der Ordnereigenschaften ändern, erhält dieser auch eine neue Revisionsnummer. Nach der Verzweigung gibt es für den Ordner ein neues Objekt im Repository und er hat auf Ordnerebene keine Zugriffsrechte mehr.
- Wenn ein Ordner bei einer Änderung nicht verzweigt wird und Sie eine der Ordnereigenschaften ändern, erhält dieser eine neue Revisionsnummer, aber es wird kein neues Objekt erstellt. In diesem Fall bleiben die Zugriffsrechte für den Ordner in beiden Ansichten bestehen. Da beide Ansichten weiterhin dasselbe Objekt beinhalten, wirken sich Änderungen, die Sie an den Zugriffsrechten des Ordners in einer Ansicht vornehmen, auch in der anderen Ansicht aus.

Verwandte Konzepte

Übersicht über Sicherheitsstrategien
Zugriffsrechte gewähren

Verwandte Verfahrensweisen

Zugriffsrechte und Gruppenberechtigungen verwalten

Zugriffsrechte auf Elementebene gewähren

Obwohl Zugriffsrechte für einzelne Elemente festgelegt werden können, wird dies selten getan. Wenn es beispielsweise sehr wichtig ist, dass eine Datei nur einer bestimmten Person angezeigt wird, kann diese Person individuelle Zugriffsrechte für diese Datei erhalten. Standardmäßig können jedoch auch der Eigentümer der Datei und alle Mitglieder einer Gruppe mit den entsprechenden Berechtigungen die Datei anzeigen.

Um sicherzustellen, dass nur eine bestimmte Person auf die Datei zugreifen kann, müssen Sie die Funktion deaktivieren, mit der der StarTeam-Server nach Berechtigungen sucht. Der Zugriff auf Objekte würde dann allein durch die festgelegten Zugriffsrechte gesteuert.

Ähnlich wie Ordner behalten Elemente in einer Unteransicht die Zugriffsrechte, über die sie in der übergeordneten Ansicht verfügten, solange sie sich nicht in neue Objekte verzweigen. Sobald Verzweigungen bei Elementen auftreten, verlieren diese ihre Zugriffsrechte.

Ordner oder Elemente verschieben

Wenn Sie einen Ordner oder ein Element verschieben, bleiben die auf Ordner- oder Elementebene festgelegten Zugriffsrechte an der neuen Position bestehen. Wenn Sie beispielsweise den Ordner "User Manuals" aus der StarDraw-Ansicht in eine andere Ansicht verschieben, hat er in der neuen Ansicht dieselben Zugriffsrechte auf Ordnerebene wie in der Ansicht "StarDraw". Er verfügt außerdem über dasselbe Verhalten, d. h., dass er sich bei einer Änderung verzweigt bzw. nicht verzweigt.

Ordner oder Elemente gemeinsam nutzen

Wenn Sie einen Ordner oder ein Element gemeinsam nutzen, bleiben die auf Ordner- oder Elementebene festgelegten Zugriffsrechte bestehen, bis der Ordner oder das Element verzweigt wird.

Wenn Sie einen Ordner oder ein Element gemeinsam nutzen, ändert sich möglicherweise das Verhalten. Nach der Freigabe zur gemeinsamen Nutzung ändert sich das Verhalten automatisch in **Verzweigen bei Änderung**, auch wenn das entsprechende Auswahlfeld an der ursprünglichen Position deaktiviert war. Ob das Auswahlfeld **Verzweigen bei Änderung** aktiviert oder deaktiviert ist, hängt von folgender Eigenschaftseinstellung für die Zielansicht ab: **Bei Änderung von gemeinsam genutzten Elementen in der Ansicht verzweigen**.

Bei einer Verzweigung des Ordners oder Elements an der neuen Position wird im Repository ein neues Objekt erstellt, für das zunächst keine Zugriffsrechte auf Ordner- oder Elementebene vorhanden sind.

Verwandte Konzepte

Übersicht über Sicherheitsstrategien
Zugriffsrechte gewähren

Verwandte Verfahrensweisen

Zugriffsrechte und Gruppenberechtigungen verwalten

Zugriffsrechte verweigern

StarTeam überprüft die gewährten Rechte für einen bestimmten Knoten auf einer bestimmten Ebene, bis ein Datensatz gefunden wird, der dem Benutzer die Berechtigung zum Ausführen einer Operation gewährt oder bis alle Datensätze zu gewährten Rechten überprüft wurden und kein entsprechendes Recht gefunden wurde. Wenn dem Benutzer das Ausführen einer Operation durch die Mitgliedschaft in einer Gruppe nicht ermöglicht, durch die Mitgliedschaft in einer zweiten Gruppe aber dennoch gewährt wird, kann der Benutzer die Operation ausführen. Wenn dem Benutzer das Ausführen einer Operation für diesen Knoten jedoch mithilfe eines Datensatzes mit verweigerten Rechten verweigert wird, kann der Benutzer diese Operation nicht ausführen. Die Anwendung ignoriert gewährte Zugriffsrechte für denselben Knoten, die dem Benutzer das Ausführen der Operation gestattet hätten.

Überlegungen zu Datensätzen mit verweigerten Rechten

Datensätze mit verweigerten Rechten werden nur selten eingesetzt. Sie können jedoch verwendet werden, um Ausnahmen für aktuell zugewiesene Rechte zu definieren. Beachten Sie folgende Punkte:

- Datensätze mit verweigerten Rechten müssen Datensätzen mit gewährten Rechten vorangestellt werden. Der Grund hierfür ist, dass die Anwendung auf derselben Ebene nicht nach weiteren Rechten für einen Knoten sucht, nachdem es ein Recht gefunden hat, das einem Benutzer das Ausführen einer Operation gewährt. Das verweigerte Recht wird dann nicht mehr gefunden. Daher wird dem Benutzer die Ausführung der Operation gewährt.
- Wenn Sie einen Datensatz zum Gewähren von Rechten erstellen, in dem kein Auswahlfeld aktiviert ist, ist dies nicht dasselbe wie das Erstellen eines Datensatzes zum Verweigern von Rechten, in dem alle Auswahlfelder aktiviert sind, obwohl durch beide Datensätze Benutzern und Gruppen die Durchführung derselben Operationen verweigert wird.
- Gruppenberechtigungen haben Vorrang vor Datensätzen mit gewährten oder verweigerten Rechten.

Datensätze mit verweigerten Rechten für Projekte

Bevor Sie ein Projekt permanent aus StarTeam löschen, möchten Sie es möglicherweise zunächst vor Benutzern *verbergen*. Wenn Sie einen Datensatz mit verweigerten Rechten auf Projektebene für die Gruppe **Alle Benutzer** (oder für eine andere übergeordnete Benutzergruppe, die Zugriff auf das Projekt hat) erstellen, wird diesen Benutzern die Berechtigung verweigert, das Projekt anzusehen. Es ist in der Ansicht nicht sichtbar und die Gruppe hat keinen Zugriff darauf.

Verwandte Konzepte

Übersicht über Sicherheitsstrategien
Zugriffsrechte gewähren

Verwandte Verfahrensweisen

Zugriffsrechte und Gruppenberechtigungen verwalten

Allgemeine Regeln für Zugriffsrechte

Beachten Sie beim Gewähren von Zugriffsrechten die folgenden allgemeinen Regeln:

- Zugriffsrechte können außer Kraft gesetzt werden, wenn ein Benutzer Eigentümer des Objekts ist. In der Regel ist der Eigentümer die Person, die das Objekt erstellt hat.
- Zugriffsrechte können durch Berechtigungen außer Kraft gesetzt werden, die einer Gruppe gewährt werden, in der der Benutzer Mitglied ist. Diese Berechtigungen werden vom Server für einzelne Gruppen festgelegt. Standardmäßig verfügt die Gruppe **Administrators** über alle Berechtigungen.
- Zugriffsrechte sollten auf der höchstmöglichen Ebene festgelegt werden.
- Der Client überprüft Zugriffsrechte von der untersten Ebene (Elementebene) bis zur höchsten Ebene (Projektebene).
- Wenn für einen Knoten Rechte gewährt werden, sollten Sie für alle Gruppen, die auf dieser Ebene Zugriff auf das Projekt benötigen, Rechte für diesen Knoten gewähren. Die Gruppe **Administrators** sollte über Rechte für alle Knoten verfügen, damit Administratoren weiterhin Zugriffsrechte ändern können, wenn Berechtigungen ignoriert werden.
- Wenn ein Benutzer oder eine Gruppe Zugriffsrechte für einen Knoten erhält, werden allen Benutzern oder Gruppen, denen die entsprechenden Rechte nicht gewährt wurden, alle Zugriffsrechte auf dieser Ebene für den Knoten verweigert.
- Alle Ansichten innerhalb eines Projekts verfügen über dieselben Zugriffsrechte auf Projektebene.
- Wenn Sie eine Unteransicht aus einer vorhandenen Ansicht ableiten, verfügt die neue Ansicht über keine Zugriffsrechte auf Ansichtsebene. Ordner und Elemente, die bereits in der übergeordneten Ansicht vorhanden waren, behalten die auf Ordner- oder Elementebene festgelegten Zugriffsrechte der übergeordneten Ansicht. Durch das Ändern der Zugriffsrechte in der über- oder der untergeordneten Ansicht werden diese auch in der anderen Ansicht geändert, da die Rechte für dasselbe Objekt geändert werden. Wenn die Ordner oder Elemente in der über- oder der untergeordneten Ansicht verzweigt werden, können sie über unterschiedliche Zugriffsrechte verfügen, da es sich um unterschiedliche Objekte handelt.
- Ordner, die aus einer Ansicht in eine andere Ansicht verschoben oder freigegeben werden, behalten in der neuen Ansicht alle Zugriffsrechte, die auf Ordnerebene festgelegt wurden. Nach einer Verzweigung gehen die Zugriffsrechte auf Ordnerebene jedoch verloren.
- Elemente, die aus einer Ansicht in eine andere Ansicht verschoben oder freigegeben werden, behalten in der neuen Ansicht alle Zugriffsrechte, die auf Elementebene festgelegt wurden. Nach einer Verzweigung gehen die Zugriffsrechte auf Elementebene jedoch verloren.
- Vermeiden Sie das Festlegen von Zugriffsrechten auf Elementebene.
- Vermeiden Sie das Verweigern von Zugriffsrechten. Wenn Sie dennoch Rechte verweigern müssen, sollten Sie folgende Regeln beachten: a) im Dialogfeld **Zugriffsrechte** sollte ein Knoten niemals ausschließlich über Datensätze zu verweigerten Rechten verfügen und b) stellen Sie für einen Knoten sicher, dass die Datensätze mit verweigerten Rechten den Datensätzen mit gewährten Rechten immer vorangestellt werden.

Verwandte Konzepte

Übersicht über Sicherheitsstrategien
Zugriffsrechte gewähren

Verwandte Verfahrensweisen

Zugriffsrechte und Gruppenberechtigungen verwalten

Zugriffsrechte und Gruppenberechtigungen

Wenn Benutzer sich bei einer Serverkonfiguration anmelden, werden sie einzeln über ihre Benutzernamen und als Mitglieder der Gruppe, der sie angehören, identifiziert. Die Anwendung speichert diese Informationen in einem Zugriffs-Token für jeden Benutzer. Während Benutzer Operationen an Anwendungsobjekten (Projekten, Ansichten, Ordnern und Elementen) ausführen, überprüft die Anwendung diese Token und die Zugriffsrechte für die Objekte, an denen die Benutzer die Operationen ausführen. Die Anwendung überprüft die Zugriffsrechte auf verschiedenen Ebenen. Das Recht, auf ein Objekt zuzugreifen, beginnt mit dem Dialogfeld **Systemrichtlinie**, auf das Sie über das Serveradministrations-Tool zugreifen können.

Wenn die Gruppenberechtigungen berücksichtigt werden, überschreiben sie alle an anderen Orten erstellten Berechtigungen und sind diesen übergeordnet. Berechtigungen sind Gruppeneigenschaften, die im Register **Berechtigungen** des Dialogfelds **Gruppeneigenschaften** auf dem Client festgelegt werden. Ein Benutzer erhält genau die Berechtigungen, die der Gruppe zugewiesen sind, der er angehört. Wenn der Benutzer zwei Gruppen angehört und einer Gruppe Berechtigungen zugewiesen werden, die der anderen nicht zugewiesen sind, erhält der Benutzer diese Berechtigungen trotzdem. Im Register **Mitgliedschaft** des Dialogfelds **Eigenes Konto** werden die Informationen zur Gruppenmitgliedschaft des angemeldeten Benutzers angezeigt.

Nachdem die Anwendung die Gruppenberechtigungen überprüft hat, werden die Zugriffsrechte für einzelne Objekte geprüft. Die Einstellungen in den Dialogfeldern **Zugriffsrechte** für Projekte, Ansichten, Ordner und einzelne Elemente gewähren oder verweigern Benutzern oder Gruppen das Ausführen von Operationen auf genau diesen Ebenen. Beachten Sie stets, dass Zugriffsrechte, die Sie für Benutzer oder Gruppen auf einer bestimmten Ebene im Dialogfeld **Zugriffsrechte** vergeben, den von diesen Rechten ausgenommenen Benutzern und Gruppen alle Zugriffsrechte für die entsprechende Ebene verweigern.

Es sei noch darauf hingewiesen, dass ein Benutzer, der ein Objekt anzeigen kann und nicht am Ausführen einer Operation durch bestimmte Zugriffskriterien gehindert wird, alle Aktionen ausführen kann, die ein Datensatz mit gewährten Rechten zulässt. Dabei spielt es keine Rolle, ob es sich um einen Einzelbenutzer oder ein Mitglied einer Gruppe handelt. Die einzige Ausnahme steht in Zusammenhang mit Berechtigungen.

Verwandte Konzepte

Übersicht über Sicherheitsstrategien
Zugriffsrechte gewähren

Verwandte Verfahrensweisen

Zugriffsrechte und Gruppenberechtigungen verwalten

StarTeam SDK-Verbindungssteuerung

StarTeam 2009 Server ermöglicht Administratoren, die Client-Anwendungen zu optimieren, die eine Verbindung zum Server aufnehmen können, indem Sie eine neue `app-control.xml`-Datei anpassen. Diese Funktion verhindert, dass unerwünschte SDK-Anwendungen eine Verbindung zum Server herstellen und Serverressourcen binden.

Hinweis: Dies ist grundsätzlich eine administrative, aber keine Sicherheitsmaßnahme.

Konfigurationsdatei "app-control.xml"

Der Server sucht nach einer neuen Konfigurationsdatei mit dem Namen **app-control.xml**, die sich im Unterverzeichnis `AppControl` unter dem Stammverzeichnis des StarTeam-Repositorys befindet. Wenn eine neue Konfiguration erstellt wird, erzeugt StarTeam 2009 Server diese Datei aus der Vorlage `app-control.xml`, die sich im Verzeichnis `AppControl` unter dem Server-Installationsverzeichnis befindet.

Die Konfigurationsdatei `app-control.xml` enthält, falls vorhanden, einen Regelsatz. Jede Regel weist den Server an, die eingehenden Client-Verbindungen zu testen, um sicherzustellen, dass eine oder mehrere der folgenden Bedingungen erfüllt sind:

- Das StarTeam SDK ist neuer oder gleich einer bestimmten Version.
- Der Anwendungsname, der Name des verbindenden Benutzers und/oder der Client-Workstation-Name müssen mit einem angegebenen Textmuster übereinstimmen.

Der Server testet jede eingehende Client-Verbindung anhand der Regeln in der Datei `app-control.xml`, bis eine Übereinstimmung gefunden wird oder die Regelliste abgearbeitet ist. Sobald eine Übereinstimmung gefunden wird, werden keine weiteren Prüfungen mehr durchgeführt und die Sequenz für das Verbindungs-Handshake wird fortgesetzt. Wird keine Übereinstimmung gefunden, wird die Verbindung verweigert. Wenn die Datei `app-control.xml` nicht im Verzeichnis `AppControl` vorhanden ist, erlaubt der Server allen unterstützten Client-Anwendungen, eine Verbindung herzustellen.

app-control.xml - Struktur und Regelsyntax

`app-control.xml` ist eine XML-Datei. Das Stamm-XML-Element muss `StarTeamApplications` heißen und ein `version`-Attribut mit dem Wert `1.0` enthalten. Beispiel: `<StarTeamApplications version="1.0">`

Der Server erkennt die folgenden Elemente direkt unter dem Stammknoten

AllowedApp

`AllowedApp:` Dies ist das Haupt-Regelelement. Es muss ein `Namensattribut` haben, das das Textmuster für den Namen der Client-Anwendung angibt (wie z. B. "Client-Identifikations-String"). Das Textmuster kann ein Sternchen ("*") als Platzhalter enthalten. Neben dem `Namensattribut` kann dieser Knoten optional ein oder mehrere der folgenden Attribute angeben:

- `MinimumSDKVersion:` gibt die Mindestversion des StarTeam SDK an, mit der die Client-Anwendung gebaut wird. Das Format dieses Felds ist `nn.nn.nn.nn`, wobei `nn` eine nicht-negative Zahl ist. Es müssen nicht alle Punktnummern angegeben werden, beispielsweise lässt `MinimumSDKVersion=”10.4”` die Versionen `10.4.x.y` und höher (`10.5`, `11.0` usw.) zu.
- `WorkStationID:` Falls festgelegt, wird damit das Textmuster für den Namen des Client-Computers angegeben.

- `Name:` Falls festgelegt, wird damit das Textmuster für den StarTeam-Benutzernamen angegeben.

Wenn kein optionaler Parameter gesetzt ist, testet der Server das entsprechende Verbindungsattribut nicht.

AppDefault

`AppDefault:` Dies ist ein optionales Element, das zum Angeben der Standardwerte für einen der Parameter verwendet werden kann, die unter `AllowedApp` aufgelistet sind. Die Syntax dieses Elements entspricht der Syntax für `AllowedApp` mit der Ausnahme, dass das `Namensattribut` keinen Standardwert haben kann. Für `MinimumSDKVersion`, `WorkStationID` und `UserName` können Standardwerte angegeben werden.

Speicherorte für die Datenspeicherung

Dieser Abschnitt enthält konzeptionelle Themen, die sich mit dem Speichern von Daten in StarTeam befassen.

In diesem Abschnitt

Übersicht über die Datenspeicherung

Beim Erstellen einer neuen Serverkonfiguration richtet StarTeam-Server eine Reihe von Ordnern für das Speichern von Protokolldateien, Anhängen, Archivdateien usw. ein. Dieses Thema beschreibt den Speicherort und den Zweck von Dateien und Ordnern, die im Native-II-Datenspeicher enthalten sind.

Native-II-Datenspeicher

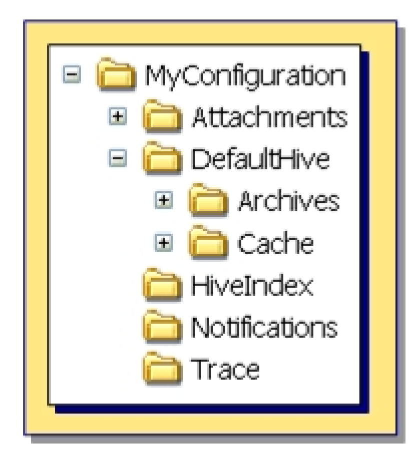
Alle Serverkonfigurationen, die vor StarTeam Server 2005 erstellt wurden, haben Native-I-Datenspeicher für die Datenspeicherung verwendet. In allen mit StarTeam Server 2005 oder späteren Versionen erstellten Serverkonfigurationen werden neue Archivdateien ausschließlich in Native-II-Datenspeichern abgelegt. Ab Version StarTeam 2006 verwenden Serverkonfigurationen nur Nativ-II Datenspeicher für die Archivdateispeicherung.

Der Native-II-Datenspeicher verbessert die Leistung von StarTeam und ermöglicht das Speichern viel größerer Dateien als in den Vorgängerversionen von StarTeam. Für StarTeam verfügt Ihre Serverkonfiguration nur über Native-II-Archivdateien, d. h. dass Backups ausgeführt werden können, ohne den Server herunterfahren zu müssen.

Warnung: Sie sollten Repository-Dateien ausschließlich über StarTeam-Server löschen oder ändern.

Repositorys

Die folgende Abbildung zeigt eine Serverkonfiguration, deren Repository-Pfad mit einem Laufwerksbuchstaben beginnt (nicht in Abbildung enthalten) und mit einem Ordner namens *MyConfiguration* endet. Das Repository enthält die Unterordner *Attachments*, *DefaultHive*, *HiveIndex*, *Notifications*, und *Trace* , wie in der untenstehenden Abbildung dargestellt. Der Ordner *DefaultHive* enthält die Unterordner *Archives* und *Cache*.



Der Name der Serverkonfiguration kann ebenfalls *MyConfiguration* lauten. Der Repository-Pfad ist ein allgemeiner Pfad für die anfängliche Speicherung einer Reihe von Objekten, von denen die meisten später unabhängig voneinander an andere Speicherorte verschoben werden können.

Protokolldateien und Ordner

Der Ordner des Repository-Pfads, z. B. *MyConfiguration* im gezeigten Beispiel, ist der Stammordner der im Folgenden aufgeführten Objekte.

Serverprotokolldateien	Bei jedem Start einer Serverkonfiguration wird eine neue Serverprotokolldatei erstellt. Weitere Informationen hierzu finden Sie unter den Links "Sicherheitsprotokolle" und "Mit dem Serverprotokoll arbeiten" am Ende dieses Themas.

.dmp-Dateien	Der Server erstellt .dmp-Dateien, wenn Sie die Serverdiagnose zum Protokollieren von Fehlern und unerwarteten Bedingungen verwenden. In der Regel haben Sie keine .dmp- oder Trace-Dateien (werden im Folgenden unter *Der Unterordner Trace* beschrieben), wenn Sie nicht mithilfe eines Mitarbeiters des technischen Supports von Borland versuchen, ein Problem zu beheben. Weitere Informationen zur Serverdiagnose finden Sie unter dem Link "Serverprobleme diagnostizieren" am Ende dieses Themas.
Der Unterordner "Trace"	Im Unterordner "Trace" werden die Dateien gespeichert, die erzeugt werden, wenn Sie mithilfe der Serverdiagnose Serverbefehle zurückverfolgen. Weitere Informationen zur Serverdiagnose finden Sie unter dem Link "Serverprobleme diagnostizieren" am Ende dieses Themas.

Diese Objekte müssen nicht im Repository-Pfad verbleiben. Sie können den Pfad aller genannten Ordner durch Ändern des **Protokollpfads** im Serveradministrations-Tool ändern.

Weitere Informationen hierzu finden Sie unter dem Link "Serverkonfigurationen erstellen" am Ende dieses Themas.

Tipp: Diese Ordner müssen bei einem Backup nicht gesichert werden.

Ordner 'Attachments'

Der Repository-Pfad, z. B. der Ordner *MyConfiguration* im gezeigten Beispiel, verfügt außerdem über den Unterordner *Attachments*.

Der Ordner *Attachments* enthält Unterordner mit den an bestimmten Elementtypen angehängten Dateien. Der Ordner *Change_Attachments* enthält beispielsweise Dateien, die an Änderungsanforderungen angehängt sind.

Sie können den Pfad zum Ordner *Attachments* separat ändern, indem Sie den **Pfad für Anhänge** im Register **Allgemein** des Dialogfelds **Server konfigurieren** (**Tools** ▸ **Administration** ▸ **Server konfigurieren**) im Serveradministrations-Tool ändern.

Tipp: Dieser Ordner muss kein Unterordner des Repository-Pfads sein. Diese Ordner müssen bei einem Backup gesichert werden.

Native-II-Datenspeicher - Ordner

Für Serverkonfigurationen ist der Repository-Pfad zudem das anfängliche Home-Verzeichnis mehrerer Ordner, die vom Native-II-Datenspeicher verwendet werden, um Archivdateien und Informationen über diese zu speichern. Der *Standard-Hive*-Ordner enthält zwei Unterordner: "Archives" und "Cache". Diese Ordner werden im Folgenden beschrieben.

HiveIndex	Im Ordner *HiveIndex* wird die Datei `hive-index.xml` gespeichert, die die Eigenschaften der von der Serverkonfiguration verwendeten Hives enthält. Den Pfad zum Ordner *HiveIndex* können Sie durch Anpassen des Repository-Pfads in der Datei `starteam-server-configs.xml` ändern. Diese Änderung sollten Sie nur vornehmen, wenn dies notwendig ist, z. B. wenn ein Laufwerk beschädigt ist. **Tipp:** Der Ordner *HiveIndex* muss bei einem Backup gesichert werden.
DefaultHive	Wenn Sie beim Erstellen einer Serverkonfiguration alle Vorgabe-Einstellungen akzeptieren oder eine aktualisierte Serverkonfiguration starten, ohne einen Hive zu erstellen, legt StarTeam-Server automatisch den Ordner *DefaultHive* an. Dieser Ordner ist ein Unterordner des Repository-Pfads und wird beim ersten Start der Serverkonfiguration erstellt.

	Unabhängig davon, ob der erste Hive *DefaultHive* heißt oder nicht, verfügt jede Serverkonfiguration über mindestens einen Hive. Sie können mehrere Hives anlegen. Jeder Hive hat einen Archiv- und einen Cache-Pfad. Eine einfache, aber nicht vorgeschriebene Namenskonvention ist die Verwendung von *DefaultHive*. Der Name des Hives wird der Name eines Ordners mit zwei Unterordnern: *Archives* und *Cache*. Sie können den Pfad dieser Ordner jedoch beliebig verändern. Sie müssen sich nicht auf demselben Laufwerk befinden.
Unterordner "Archives"	Dieser Ordner enthält Dateirevisionen in Archivdateien, die komprimiert sein können.
Unterordner "Cache"	In diesem Ordner werden unkomprimierte Versionen der Archivdateien gespeichert. Er verfügt über zwei Unterordner namens *Temp* und *Deltas*. Unter *Temp* werden neu zu StarTeam hinzugefügte Dateien und neu eingecheckte Dateirevisionen gespeichert. In *Deltas* werden die Unterschiede zwischen den Arbeitsdateien und den aktuellen Revisionen gespeichert, wenn ein Benutzer möchte, dass die Datenübertragung über langsame Verbindungen optimiert wird. Diese Option ist auf dem Client im Register **Datei** des Dialogfelds **Persönliche Optionen** verfügbar.

Verwandte Konzepte

Sicherheitsprotokolle
Native-II-Datenspeicher und Hives

Verwandte Verfahrensweisen

Mit dem Serverprotokoll arbeiten
Serverprobleme diagnostizieren
Serverkonfigurationen erstellen
Optionen für die Datenspeicherung konfigurieren

Native-II-Datenspeicher und Hives

Der Native-II-Datenspeicher verbessert die StarTeam-Leistung (im Vergleich mit der als Native-I bezeichneten, alten Datenspeicherstruktur) und ermöglicht es Ihnen, viel größere Dateien als in früheren Versionen von StarTeam zu speichern. Zudem ermöglichen es Ihnen Serverkonfigurationen, die Native-II-Archivdateien verwenden, Backups ohne Herunterfahren des Servers auszuführen. StarTeam-Serverkonfigurationen unterstützen nur Native-II-Datenspeicher.

In diesem Thema wird Folgendes beschrieben:

- Leistung des Native-II-Datenspeichers
- Hives
- Archiv- und Cache-Struktur
- Delta-Speicherung

Leistung des Native-II-Datenspeichers

In den folgenden Abschnitten wird erklärt, wie StarTeam Dateien hinzufügt, eincheckt und auscheckt.

Dateien hinzufügen

Um eine Datei zum Native-II-Datenspeicher hinzuzufügen, speichert StarTeam-Server die Revision in einem temporären Ordner, berechnet den MD5-Wert des Inhalts und prüft, wie gut sich die Datei komprimieren lässt. Wenn der Komprimierungsfaktor bei 10 % oder höher liegt, verschiebt der Server die komprimierte Version in das Hive-Archiv und die unkomprimierte Version in den Hive-Cache. Wenn die Revision sich nicht optimal komprimieren lässt, wird die unkomprimierte Version in das Hive-Archiv verschoben.

StarTeam konvertiert den MD5-Wert in einen Hex-String und verwendet diesen als Namen für die Archivdatei. Wenn die Archivdatei komprimiert ist, erhält sie die Erweiterung .gz. Wenn bereits eine Archivdatei mit diesem Namen vorhanden ist, wird keine neue Archivdatei erstellt, obwohl die Eigenschaften der StarTeam-Datei Angaben zu dem Hive, in dem die Revision gespeichert ist, zur Komprimierung und den Namen der Archivdatei enthalten.

Eincheckvorgänge

Um eine Dateirevision in den Native-II-Datenspeicher einzuchecken, speichert der StarTeam-Server die Revision in einem temporären Ordner im Hive der nächsten Hive-Rotation. Anschließend berechnet der Server den MD5-Wert des Inhalts. Wenn bereits eine Archivdatei mit dem richtigen Namen im Hive vorhanden ist, wird keine neue Archivdatei erstellt, obwohl die Eigenschaften der Dateirevision aktualisiert werden. Andernfalls wird eine neue Archivdatei erstellt. Beachten Sie, dass in einem Hive niemals zwei Dateien gespeichert werden, deren Inhalt identisch ist.

Wenn die StarTeam-Datei anfänglich als gut zu komprimierende Datei eingestuft wurde, komprimiert StarTeam die Dateirevision und legt sie mit der Erweiterung .gz im Archiv des Hives ab. Die unkomprimierte Version wird im Cache des Hives abgelegt. Wenn die Datei nicht gut zu komprimieren ist, wird sie unkomprimiert im Archiv des Hives abgelegt.

Auscheckvorgänge

Um eine Dateirevision aus einem Native-II-Datenspeicher abzurufen, prüft StarTeam-Server die Hive-ID der Revision und den Namen der Archivdatei. Anschließend ruft der Server die Dateirevision aus dem Cache- oder Archiv-Ordner des angegebenen Hives ab. Bei 2005- und späteren Clients wird die Archivdatei direkt versendet. Diese Clients können die Archivdatei ggf. entpacken.

Hives

Ein Hive bezeichnet den Speicherort auf dem Computer, an dem StarTeam-Server die Archivdateien und den Cache speichert. Diese Elemente sind in den Ordnern *Archives* und *Cache* enthalten. Wenn Sie beispielsweise eine Serverkonfiguration namens *MyConfiguration* erstellt und im Stammverzeichnis von Laufwerk `C:\` abgelegt haben, generiert StarTeam-Server standardmäßig einen Ordner unter `C:\MyConfiguration` namens *DefaultHive* , der die Unterordner *Archives* und *Cache* enthält. Der Ordner *DefaultHive* und seine Unterordner stellen den Hive dar.

Native-II-Datenspeicher von StarTeam-Server können eine beliebige Anzahl Hives haben, die jeweils über eigene Archiv- und Cache-Ordner verfügen. Sobald sich ein Hive füllt, können Sie einen weiteren hinzufügen, ohne Datenspeicherorte ändern oder Archivdateien verschieben zu müssen. Unternehmen mit großen Dateien oder einer großen Anzahl von Dateien können von vornherein mehrere Hives einsetzen. Sie können die Archiv- und Cache-Ordner sogar auf unterschiedlichen Laufwerken ablegen (dies wird empfohlen).

Native-II-Datenspeicher speichern komplette Dateirevisionen (auch wenn die Archivdatei komprimiert ist). Dies bedeutet, dass der Native-II-Datenspeicher letztendlich mehr Speicherplatz benötigt, allerdings können Sie die Revisionen unter Verwendung von Hives zur Speicherung über mehrere Laufwerke oder Volumes verteilen. Diese Flexibilität bei der Zuweisung des Speicherplatzes erweist sich nach einiger Zeit, d. h. wenn die Hives voll werden, als großer Vorteil.

Wenn eine Serverkonfiguration über mehrere Hives verfügt, speichert der Server die Dateien den einzelnen Hives der Reihe nach hinzu, bevor er wieder den Archivpfad des ersten Hives verwendet. Wenn ein StarTeam-Client auf einen StarTeam-Server zugreift und eine StarTeam-Serverkonfiguration über mehrere Hives verfügt, speichert der Server Dateien der Reihe nach. Er stellt jedoch zunächst sicher, dass kein Hive bereits über diese Datei verfügt, bevor der Client versucht, die Datei auf dem Server abzulegen.

Wenn Sie eine Serverkonfiguration erstellen, verfügt sie automatisch über mindestens einen Hive (entweder über den Standard-Hive oder über einen benutzerdefinierten Hive). Um den für diese Serverkonfiguration verfügbaren Speicherplatz zu erweitern, können weitere neue Hives mithilfe des **Hive-Managers** hinzugefügt werden. Wenn Sie remote auf eine Serverkonfiguration zugreifen, können Sie die Hives während der Ausführung der Serverkonfiguration erstellen, da die Konfiguration bereits über einen zunächst vorgegebenen Pfad verfügt, auch wenn dieser auf einen *DefaultHive* im Repository-Pfad verweist. Weitere Informationen zum Erstellen von Hives finden Sie unter dem Link "Neue Hives erstellen" am Ende dieses Themas.

Sie können auch den **Hive-Manager** verwenden, um einen einzelnen Archiv- und/oder Cache-Pfad für einen Hive zu ändern. Sie sollten solche Änderungen nur vornehmen, wenn der Hive verschoben werden muss. Beispielsweise können Sie einen Hive verschieben, weil ein Laufwerk beschädigt ist. Außerdem müssen Sie den Inhalt des Archivpfads des Hives an den neuen Speicherort kopieren. Weitere Informationen hierzu finden Sie unter dem Link "Den Archivpfad anpassen" am Ende dieses Themas.

Hinweis: Borland empfiehlt, die Volumes *Archives* und *Cache* aus einer Serverkonfiguration nicht den Volumes *Archive* und *Cache* aus einer anderen Serverkonfiguration zuzuordnen. Anderenfalls werden die Schwelleneinstellungen für die Ordner *Archives* nicht genau berechnet. Dies liegt daran, dass der Server beim Start einer Serverkonfiguration den verfügbaren Speicherplatz überprüft und den zurückgegebenen Wert im Cache-Speicher ablegt. Wenn Dateien hinzugefügt oder entfernt werden, passt der Server den verfügbaren Speicherplatz zur Bereinigung des Cache-Speichers an und ermittelt, ob der Schwellenwert überschritten wurde. Zur Leistungssteigerung wird der Schwellenwert im Cache-Speicher abgelegt und nicht jedes Mal neu überprüft, wenn eine Datei hinzugefügt oder entfernt wird. Der Schwellenwert wird vom Server als Anhaltspunkt verwendet, um zu ermitteln, ab wann keine Dateien mehr in einem bestimmten Hive abgelegt werden sollten. Der Schwellenwert ist also kein absoluter Grenzwert. Wenn es Anzeichen dafür gibt, dass der Schwellenwert ausgehend von dem im Cache gespeicherten Wert für den verfügbaren Speicherplatz überschritten wurde, führt der Server außerdem eine weitere Überprüfung durch und fragt das Dateisystem wie beim Start ab, um sicherzustellen, dass der aktuelle Wert für den verfügbaren Speicherplatz korrekt ist; erst dann werden keine weiteren Dateien mehr in einem Hive abgelegt.

Entsprechend empfiehlt Borland, da der Schwellenwert für jede Serverkonfiguration einzeln protokolliert wird, dass die Hives einzelner Serverkonfigurationen auf

voneinander unabhängige Volumes verweisen sollten, damit die Berechnung des Schwellenwertes so genau wie möglich ist (und dadurch das Dateisystem weniger oft auf verfügbaren Speicherplatz überprüft wird).

Archiv- und Cache-Struktur

Die Struktur der Archiv- und Cache-Pfade aller Hives ist gleich. Sie ähnelt der von den StarTeam-Clients verwendeten Strukturen zum Speichern von Dateistatusinformationen.

Die im Archiv- und im Cache-Ordner gespeicherten Dateien werden von StarTeam in Unterordner verteilt. So können Dateien einfacher gefunden und verwaltet werden. Der Name der Unterordner, in dem StarTeam eine Dateirevision speichert, basiert auf den ersten Zeichen des Namens der Archivdatei.

Angenommen, der Inhalt einer Dateirevision hat den MD5-Wert `01fc3c4ac5e0e92cc707f30fb73a0726`. Wenn der Benutzer den Archivpfad `C:\DefaultHive\Archives` ausgewählt hat, hat die genannte Revision einen der folgenden Archivpfade, je nachdem, ob die Archivdatei komprimiert ist:

`C:\DefaultHive\Archives\01\f\01fc3c4ac5e0e92cc707f30fb73a0726`

`C:\DefaultHive\Archives\01\f\01fc3c4ac5e0e92cc707f30fb73a0726.gz`

Hinweis: Bei einem Backup müssen die Archivpfade aller Hives hinzugefügt werden (z. B. `C:\DefaultHive\Archives`).

Delta-Speicherung

StarTeam verwendet Deltas, um die Datenübertragung über langsame Verbindungen zu optimieren. Um diese Funktion verwenden zu können, müssen Benutzer die persönliche Option **Für langsame Verbindungen optimieren** festlegen, die auf dem Client im Register **Datei** des Dialogfelds **Persönliche Optionen** verfügbar ist. Wenn ein Benutzer dann eine neue Revision einer Datei auscheckt, die sich bereits in seinem Arbeitsordner befindet, erkennt der Server die Revisionsnummer der Arbeitsdatei und versendet nur die Änderungen zwischen dieser Revision und der auszucheckenden Revision.

StarTeam-Server speichert alle Deltas für die spätere Verwendung im Ordner *Deltas*, einem Unterordner des Ordners *Cache*, der sich auf jedem Hive befindet. Die Datei mit dem Delta erhält einen Namen, der die Namen der zwei Archivdateien miteinander kombiniert, die zum Erzeugen der Daten verwendet wurden. Angenommen, die auf der Festplatte des Clients gespeicherte Revision hat den MD5-Wert

`7f46c2bb9602fe972d952f4988ab85cd`

und die angeforderte Revision hat den MD5-Wert

`7f46c2bb9602fe972d952f4982ab35aa`

Der Server erzeugt ein Delta zwischen diesen zwei Revisionen mit folgender Bezeichnung:

`7f46c2bb9602fe972d952f4988ab85cd.7f46c2bb9602fe972d952f4982ab35aa`

Tipp: Weitere Informationen zum Festlegen der persönlichen Optionen auf dem Client finden Sie unter dem Link "Persönliche Optionen anpassen" am Ende dieses Themas.

Verwandte Konzepte

Übersicht über die Datenspeicherung

Verwandte Verfahrensweisen

Neue Hives erstellen
Optionen für die Datenspeicherung konfigurieren
Archivpfad anpassen

Übersicht über Benutzer- und Gruppenkonfigurationen

Sie können Borland LDAP QuickStart Manager verwenden, um Benutzerdaten aus einem Verzeichnisdienst oder einer LDIF-Datei auf einen StarTeam- oder CaliberRM-Server als Benutzereigenschaften zu importieren. Sie können neue Gruppen und Benutzer auch manuell zu einer Serverkonfiguration hinzufügen. Wenn sich Benutzer bei der Anwendung anmelden, können sie nun durch ein Passwort überprüft werden, das in der Anwendung eingegeben, importiert oder über die Microsoft Active Directory Services (LDAP-Server) bezogen wurde. Dieser Vorgang ist nur möglich, wenn der Server sich in einer Domäne befindet, die der LDAP-Server als vertrauenswürdig erkennt.

In diesem Thema wird zudem Folgendes beschrieben:

- Standardgruppen
- Gruppenmitgliedschaft
- Unterstützung für Verzeichnisdienst

Standardgruppen

Neue Serverkonfigurationen haben vordefinierte Standardgruppen: "All Users", "Administrators", "System Managers" und "Security Administrators". Für diese Gruppen wurden Standardberechtigungen festgelegt, die jedoch durch Berechtigungen ersetzt werden können, die Ihrer Unternehmensrichtlinie entsprechen.

Die Benutzer der Gruppe "Administrators" verfügen anfänglich über alle Berechtigungen, wodurch sie vollständigen Zugriff auf das System haben, es sei denn, dass Berechtigungen in Ihrem System ignoriert werden. Die Gruppen "All Users", "System Managers", "Security Administrators" und "Collaboration Users" verfügen anfänglich über keinerlei Berechtigungen.

All Users	Alle Benutzer sind Mitglieder der Gruppe "All Users", da dies die Stammgruppe im Benutzer-Manager ist und alle Mitglieder einer untergeordneten Gruppe gleichzeitig auch Mitglieder ihrer übergeordneten Gruppe sind. Daher übernehmen alle Benutzer die Rechte und Berechtigungen, die dieser Gruppe zugewiesen sind.
Administrators	Diese Gruppe enthält anfänglich nur den Serveradministrator. Sie können dieser Gruppe weitere Benutzer hinzufügen, die administrative Zugriffsrechte haben. StarTeamwird mit einem Benutzerkonto bereitgestellt, für das als Benutzername und als Passwort "Administrator" vorgegeben ist. Da dies allgemein bekannt ist, sollten Sie zumindest das Passwort ändern.
System Managers	Die Benutzer in dieser anfänglich leeren Gruppe empfangen E-Mails, die an die im Benutzer-Manager angegebene Adresse gerichtet sind, wenn im Serverprotokoll ein Fehler eingetragen wird.
Security Administrators	Die Benutzer in dieser Gruppe können E-Mails zu Benutzern empfangen, deren Anmeldeversuche fehlgeschlagen sind. Diese Gruppe enthält anfänglich nur den Benutzer, der als Server-Administrator angegeben ist.

Tipp: Sie müssen immer über mehrere Benutzerkonten mit Administratorrechten verfügen. Wenn Sie als der einzige Administrator angemeldet sind und Ihr Konto aus irgendeinem Grund gesperrt wird, gibt es keine Möglichkeit, Ihr Konto zu entsperren.

Gruppenmitgliedschaft

Ein Benutzer kann Mitglied in mehreren Gruppen sein. Benutzer, die mehreren Gruppen angehören, verfügen für jede Operation über das jeweils höchste in einer ihrer Gruppenberechtigungen festgelegte Zugriffsrecht. Angenommen, Benutzer A ist Mitglied der Gruppe *All Users* und der Gruppe *Administrators* und die Gruppe

Administrators verfügt über die **Berechtigung zum Löschen von Elementen**, die Gruppe "All Users" jedoch nicht. Benutzer A kann alle Elemente der Projekte in der Serverkonfiguration löschen.

Eine Mitgliedschaft kann explizit oder implizit sein. Eine Gruppenmitgliedschaft ist in den folgenden Fällen explizit:

- Wenn die Gruppe bei der Erstellung des Benutzerkontos ausgewählt wurde.
- Wenn der Name der Gruppe im Register **Gruppenmitgliedschaft** des Dialogfelds **Benutzereigenschaften** im Serveradministrations-Tool ausgewählt wurde.

Implizite Mitgliedschaften ergeben sich aus der Position eines Benutzers in der Gruppenhierarchie. Wenn ein Benutzer Mitglied einer Untergruppe ist, ist er implizit auch Mitglied der übergeordneten Gruppe, auch wenn sein Name in der Benutzerliste der übergeordneten Gruppe nicht direkt angezeigt wird. Sie müssen das Auswahlfeld **Benutzer in allen nachfolgenden Gruppen anzeigen** aktivieren, um eine vollständige Liste der Mitglieder einer ausgewählten Gruppe anzuzeigen, die über Untergruppen verfügt.

Ein Benutzer, der sowohl Mitglied einer übergeordneten Gruppe als auch Mitglied einer Untergruppe dieser Gruppe ist, verfügt über eine implizite und eine explizite Mitgliedschaft in der übergeordneten Gruppe.

Unterstützung für Verzeichnisdienst

StarTeam ermöglicht die Passwortverifizierung mit Microsoft Active Directory. Der Active Directory-Dienst ist in Microsoft Windows Server 2003 und Microsoft Windows 2000 verfügbar. Er unterstützt die zentralisierte, sichere Verwaltung des gesamten Netzwerks. Damit Benutzer mithilfe des Verzeichnisservers validiert werden können, muss sich der Server in einer Domäne befinden, die er als vertrauenswürdig erkennt.

Sie müssen im Register **Verzeichnisdienst** des Dialogfelds **Server konfigurieren** die Option **Unterstützung für Verzeichnisdienst aktivieren** auswählen und den Speicherort sowie die Port-Nummer des Verzeichnisservers eingeben. Für jede Person, die mithilfe des Verzeichnisservers validiert werden soll, muss die Option **Über Verzeichnisdienst validieren** im Dialogfeld **Eigenschaften für den neuen Benutzer** oder **Benutzereigenschaften** ausgewählt und ein **eindeutiger Name** (wird zur eindeutigen Identifizierung eines Verzeichnisdienstbenutzers verwendet) für die Person eingegeben werden.

Auch wenn diese Einstellungen richtig sind, kann sich der Benutzer zukünftig nicht mehr anmelden, wenn der Verzeichnisserver nicht verfügbar ist. Obwohl die Unterstützung des Verzeichnisdienstes standardmäßig deaktiviert ist, kann sie jederzeit aktiviert werden. Die Server dürfen nicht aktiviert sein, wenn Sie die Unterstützung aktivieren oder deaktivieren. Wenn der Benutzer einen StarTeam-Anmeldenamen und ein Microsoft Active Directory-Passwort angibt, erkennt der StarTeam-Server, dass für den Benutzer die Passwortverifizierung durch den Verzeichnisdienst eingerichtet wurde und verwendet den **Eindeutigen Namen** und das Passwort, um die Verbindung zu Active Directory herzustellen. Sobald das Passwort überprüft wurde, kann der Benutzer auf die StarTeam-Serverkonfiguration zugreifen.

Tipp: Weitere Informationen zum Aktivieren der Verzeichnisunterstützung finden Sie unter den Links "Unterstützung für Verzeichnisdienst aktivieren" und "Benutzer einrichten" am Ende dieses Themas.

Verwandte Konzepte

Zugriffsrechte gewähren

Verwandte Verfahrensweisen

Benutzer und Gruppen verwalten
Benutzer einrichten
Unterstützung für Verzeichnisdienst aktivieren

LDAP für die Passwortverifizierung

StarTeam kann zur Passwortautorisierung auf Verzeichnisdienste zugreifen (entweder Microsoft Active Directory oder OpenLDAP). Wenn sich Benutzer anmelden, geben sie ihren StarTeam-Benutzernamen mit dem zugehörigen Verzeichnisdienst-Passwort ein. Bevor sie auf den Server zugreifen können, überprüft StarTeam die Gültigkeit der Passwörter mithilfe eines Verzeichnisdienstes.

Borland LDAP QuickStart Manager ist ein Dienstprogramm, mit dem Benutzerdaten aus einem Verzeichnisdienst oder aus einer LDIF-Datei als Benutzereigenschaften auf den StarTeam-Server importiert werden können. Mit LDAP QuickStart Manager können eindeutige Namen und andere auf StarTeam-Servern gespeicherte Verzeichnisdienstdaten einfach verwaltet werden.

Um die Benutzerauthentifizierung mithilfe eines Verzeichnisdienstes in StarTeam einzurichten, müssen Sie Optionen im Register **Verzeichnisdienst** des Dialogfelds **Server konfigurieren** festlegen. Mit diesen Optionen wird die Unterstützung für den Verzeichnisdienst aktiviert und es werden Daten für den Zugriff auf den Dienst eingegeben. Außerdem legen Sie im Benutzer-Manager Optionen für die einzelnen Benutzer fest, deren Passwörter authentifiziert werden sollen. Diese Funktion muss nicht für alle Benutzer aktiviert werden.

Der DN (Distinguished Name) wird als eindeutiger Bezeichner von Borland-Servern bei der Kommunikation mit dem Verzeichnisdienst eingesetzt. StarTeam muss beispielsweise die DNs jedes Benutzers an den Verzeichnisdienst übermitteln, um die Benutzerpasswörter zu verifizieren. DNs sind häufig lang und nicht sehr intuitiv. Einige Organisationen ändern zudem gelegentlich die DNs, wobei die manuelle Aktualisierung dieser Änderungen sehr zeitraubend sein kann.

Geben Sie beim Importieren von Benutzern mit LDAP QuickStart Manager an, ob die Passwörter neuer Benutzer von StarTeam-Server oder einem Verzeichnisdienst authentifiziert werden sollen, indem Sie entweder den Optionsschalter **Über Verzeichnisdienst validieren** oder **Über StarTeam-Server validieren** wählen. StarTeam-Server verlangen die Verzeichnisdienst-Validierung von Benutzerpasswörtern, wenn die Serverkonfiguration zum einen die Verzeichnisdienst-Validierung zulässt und zum anderen über die richtigen Verbindungseinstellungen für den Verzeichnisdienst verfügt.

Verwandte Konzepte

Richtlinien für die Serverkonfiguration

Richtlinien für die Serverkonfiguration

Im Rahmen der anfänglichen Planung besteht eine der wichtigsten Entscheidungen, die Ihre Organisation treffen muss, darin, wie viele StarTeam-Konfigurationen verwendet werden sollen. Das Verteilen von Projekten auf mehrere StarTeam-Server führt zwar zu höheren Verwaltungskosten, gleichzeitig erhöht es jedoch auch die Projektunabhängigkeit und verbessert die Leistung und die Verfügbarkeit. Indem Sie das Projektwachstum abschätzen und Wechselbeziehungen im Voraus berücksichtigen, können Sie das Aufteilen/Teilen von zu umfangreich gewordenen Konfigurationen vermeiden. Im Folgenden finden Sie einige Strategien, die Sie bei der Entwicklung des Serverbereitstellungsplans für Ihre Organisation berücksichtigen sollten.

Vorteile gemeinsam genutzter Serverkonfigurationen

Dies sind die Vorteile einer gemeinsamen Konfiguration, die von mehreren Projekten genutzt wird:

- **Transaktionale Integrität:** Da eine Konfiguration eine einzige Datenbank verwendet, sind alle Daten innerhalb derselben Konfiguration *transaktional* konsistent. Das bedeutet, dass eine Konfiguration eine Begrenzung für die Datenkonsistenz darstellt. Wenn Sie eine Konfiguration sichern und später wiederherstellen, werden alle Informationen innerhalb der Konfiguration für denselben Zeitpunkt wiederhergestellt.
- **Verknüpfen:** Elemente innerhalb derselben Konfiguration können miteinander verknüpft werden, auch dann, wenn sie sich in verschiedenen Projekten befinden. StarTeam unterstützt derzeit keine Verknüpfungen zwischen Elementen in verschiedenen Konfigurationen.
- **Freigeben und verschieben:** Elemente können freigegeben oder in einen beliebigen Ordner, eine Ansicht oder ein Projekt innerhalb derselben Konfiguration verschoben werden. Das Verschieben oder Freigeben von Elementen über Konfigurationsgrenzen hinweg wird nicht unterstützt.
- **Einfache Administration:** Administrative Tasks wie das Hinzufügen von Benutzern und Gruppen, das Anwenden von Sicherheitsmaßnahmen, das Durchführen von Backups usw. werden auf der Konfigurationsebene ausgeführt.
- **Gemeinsam genutzte Anpassungen:** Viele StarTeam-Ressourcen, wie z. B. Filter, Abfragen, benutzerdefinierte Formulare und Workflows, können auf der Konfigurationsebene definiert und von allen Projekten gemeinsam verwendet werden. (Benutzerdefinierte Formulare und Workflows können jedoch auch für einzelne Projekte oder Ansichten angepasst werden.)
- **Gemeinsam genutzte Serverkomponenten:** Alle Daten innerhalb derselben Konfiguration verwenden einen einzigen Serverprozess, eine Datenbank, einen Datenspeicher und einen Root-Cache-Agent. Neue Projekte können dynamisch hinzugefügt werden, ohne dass neue serverseitige Komponenten hinzugefügt werden.

Vorteile separater Serverkonfigurationen

Dies sind die Vorteile der Verwendung von separaten Konfigurationen für mehrere Projekte:

- **Leistung:** Bei größeren Konfigurationen dauert der Startvorgang länger, sie benötigen mehr Ressourcen und sie geben häufig umfangreichere Antworten auf Befehle zurück. Bei kleineren Konfigurationen dagegen sind weniger Daten und weniger gleichzeitige Benutzer vorhanden, daher ist ihre Leistung im Hinblick auf diese Aspekte normalerweise besser.
- **Wachstumsverwaltung:** Auch wenn Sie anfänglich mehrere Konfigurationen auf einem einzelnen Rechner platzieren, können Sie bei Bedarf einfach eine Konfiguration auf den entsprechenden Rechner verschieben.
- **Wartungsplanung:** Separate Konfigurationen können unabhängig voneinander gestartet und gestoppt werden, um Patches zu installieren, Hardware zu aktualisieren usw. Wenn eine Konfiguration offline ist, kann auf keine der darin enthaltenen Projekte zugegriffen werden.
- **Benutzerdefinierte Felder:** Benutzerdefinierte Felder werden auf der "Typ"-Ebene hinzugefügt, die den Gültigkeitsbereich der Konfigurationsebene besitzt. Dies bedeutet, dass wenn Sie ein benutzerdefiniertes Feld zu einer Änderungsanforderung hinzufügen, alle Änderungsanforderungen in der jeweiligen Konfiguration einen Wert für das Feld besitzen. Wenn daher verschiedene Teams oder Geschäftsbereiche im Hinblick auf

benutzerdefinierte Felder unterschiedliche Interessen haben, spricht dies dafür, deren Projekte in separate Konfigurationen zu platzieren.

Weitere Überlegungen zu Serverkonfigurationen

Im den folgenden Abschnitten werden zusätzliche Faktoren beschrieben, die Sie bei der Entwicklung des Serverbereitstellungsplans für Ihre Organisation berücksichtigen sollten.

Einteilungen in Geschäftsbereiche

Wenn mehrere Geschäftsbereiche ihre eigenen StarTeam-Projekte benötigen, bietet es sich in der Regel an, die StarTeam-Server gemäß diesen organisationsspezifischen Bereichen zu definieren. Dies bedeutet, dass Sie pro Geschäftsbereich oder Abteilung einen separaten StarTeam-Server bereitstellen, sodass diese auf ihre eigenen Projekte zugreifen können. Durch das Aufteilen der Server nach Geschäftsbereichen werden die separaten (und gelegentlich konkurrierenden) Anforderungen für Sicherheit, Backup-Prozesse und andere administrative Punkte isoliert. Separate Server können auch helfen, Probleme mit Eigentumsrechten zu minimieren.

Wenn Prozesse des Entwicklungslebenszyklus sich über mehrere Serverkonfigurationen erstrecken, können auf einem einzelnen StarTeam-Client mehrere Projekte geöffnet werden. Um konfigurationsübergreifenden Anforderungen zu entsprechen, kann auch das "Bereitstellen" zusammenhängender Artefakte von einem Projekt in ein anderes verwendet werden.

Optimierte StarTeam-Unterstützung für verteilt arbeitende Teams

Teammitglieder, die Zugriff auf dieselben Artefakte benötigen, sollten einen StarTeam-Server gemeinsam nutzen. Das Aufteilen eines StarTeam-Servers nur aus dem Grund, dass sich die Teammitglieder an verschiedenen Standorten befinden, ist nicht erforderlich. StarTeam ist darauf ausgelegt, dass die Arbeit mit Teams, deren Mitglieder sich an verschiedenen Orten befinden, gut funktioniert. In StarTeam wird Wert auf einen zentralisierten Konfigurationsansatz mit MPX-Publish/Subscribe-Messaging und Cache-Agenten gelegt, um geografisch verteilte Teams zu unterstützen.

Vermeidung von Partitionen für den internen/externen Zugriff

In vielen Situationen benötigen Teams sowohl hinter als auch außerhalb der Unternehmens-Firewall Zugriff auf dieselbe StarTeam-Konfiguration. In diesem Szenario wird der StarTeam-Serverprozess in der Regel im DMZ-Bereich der Firewall bereitgestellt und der Datenbankserver und der Speicherserver werden hinter der Firewall platziert. Je nach Funktionalität der Firewall kann es angebracht sein, einen dedizierten Port für den StarTeam-Server zu konfigurieren. Alternativ können Sie auf dem StarTeam-Server-Computer auch zwei Netzwerkkarten (NICs) installieren: eine für die externe und eine für die interne Kommunikation. In diesem Szenario ermöglicht StarTeam, dass bestimmte IP-Adressen (oder Adressbereiche) für den eingehenden Verkehr mit unterschiedlichen Anforderungen für die Verbindungssicherheit konfiguriert werden können.

StarTeam bietet eine SSL-ähnliche Verschlüsselung für die Befehls-API, um das Abhören von Client/Server-Traffic zu verhindern. Der gesamte MPX Message Broker- und Cache-Agent-Verkehr ist ebenfalls verschlüsselt, sodass Daten, die über öffentliche Verbindungen übermittelt werden, nicht öffentlich zugänglich sind. Wenn Sie den Zugriff auf bestimmte Teams beschränken möchten, können Sie Referenzansichten oder die Sicherheits-ACLs von StarTeam dazu verwenden, den Zugriff auf bestimmte Projekte, Ansichten, Ordner und sogar einzelne Artefakte zu beschränken. Weitere Sicherheitsfunktionen, z. B. die Verwaltung sicherer Passwörter und automatische Kontensperren, können die Sicherheit der Verwendung derselben StarTeam-Konfiguration sowohl für interne als auch für externe Benutzer weiter erhöhen.

Für Wachstum planen

Bei der Überlegung, wie viele StarTeam-Konfigurationen Sie erstellen möchten, sollten Sie für einen längeren Zeitraum im Voraus planen: mindestens für drei bis fünf Jahre. Wenn Sie die gleichzeitige Nutzung durch mehrere

Benutzer abschätzen können, stellt dies den besten Maßstab für die Kapazitätsplanung dar. Auf der heutigen Hardware (Vierfach-CPU mit 4 GB Arbeitsspeicher) unterstützt StarTeam ohne Schwierigkeiten bis zu 300 gleichzeitige Benutzer. Einige Kunden besitzen Konfigurationen, bei denen die maximale Anzahl von gleichzeitigen Benutzern bei über 400 liegt, und bei einem Kunden sind es zeitweilig sogar 600 gleichzeitige Benutzer. Bei diesen Mengen von gleichzeitigen Benutzern kommt jedoch den Anwendungstypen eine Bedeutung zu (beispielsweise sind bei Stapelanwendungen normalerweise die Anforderungen höher als bei Online-Clients). Selbst bei 300 gleichzeitigen Benutzern kann sich die Leistung in nicht akzeptablem Maße verringern, wenn eine große Anzahl von Benutzern Anwendungen ausführen, die hohe Anforderungen stellen.

Die Skalierbarkeit von Konfigurationen kann auch mit Befehlsraten gemessen werden. Sie können die Befehlsraten einer vorhandenen Konfiguration mithilfe der Server-Trace-Funktionalität messen. Der StarTeam-Server kann so eingestellt werden, dass er bei Befehlsraten zwischen 200.000 und 300.000 Befehlen pro Stunde (56 bis 83 Befehle pro Sekunde) eine angemessene Performance bietet. Bei guter Netzwerk-Infrastruktur (niedrige Latenz) wurden bereits Befehlsraten von 400.000 Befehlen pro Stunde (111 Befehle pro Sekunde) und mehr bei angemessener Performance erreicht. Wenn versucht wird, bei einer einzelnen Konfiguration höhere Werte zu erzielen, entstehen zumeist inakzeptable Antwortzeiten.

Wenn es Ihnen nicht möglich ist, die Anzahl der gleichzeitigen Benutzer oder die Befehlsraten vorauszuberechnen, können Sie "definierte" Benutzer verwenden. Die Serverauslastung ist bei der alleinigen Verwendung von definierten Benutzern jedoch schwieriger vorherzusagen. Wenn sich die Benutzer einer Benutzergruppe an unterschiedlichen Standorten befinden, liegt das Verhältnis von definierten Benutzern zu gleichzeitigen Benutzern in der Regel bei etwa 10:1. Bei 1.000 benannten Benutzern ist demnach zu Spitzenzeiten mit etwa 100 gleichzeitigen Benutzersitzungen zu rechnen. Wenn die Standorte der Benutzer weniger variieren und die Benutzer in einer oder zwei Zeitzonen konzentriert sind, ist zu erwarten, dass das Verhältnis von definierten Benutzern zu gleichzeitigen Benutzern eher bei etwa 5:1 liegt. Wenn Ihnen keine besseren Daten zur Verfügung stehen, verwenden Sie diese Näherungswerte, um die Anzahl von gleichzeitigen Benutzern zu Spitzenzeiten zu bestimmen.

Nachdem Sie Ihre Vorhersage für die nächsten drei bis fünf Jahre berechnet haben, sollten Sie einschätzen können, wie viele StarTeam-Konfigurationen für Ihren Benutzerkreis erforderlich sein werden.

Verwandte Konzepte

[Übersicht über die Serverkonfiguration]

Verwandte Verfahrensweisen

[Serverkonfigurationen erstellen]
[Dateirevisionen mit Vault Verify verifizieren]
[Gelöschte Ansichten aus Serverkonfigurationen entfernen]

Atomische Eincheckvorgänge

Alle Eincheckvorgänge in StarTeam sind atomisch. Wann immer mehrere Dateien in Folge einer einzelnen Transaktion eingecheckt werden, werden alle Dateien sowie ihre verknüpften Prozesselemente in einer Aktion aktualisiert. Wenn das Einchecken aus irgendeinem Grund fehlschlägt, wird keine der Dateien eingecheckt und der Status der verknüpften Prozesselemente wird nicht aktualisiert.

Angenommen, Benutzer A möchte alle geänderten Dateien in einen StarTeam-Ordner einchecken, aber eine der ausgewählten Dateien ist durch Benutzer B gesperrt. Aufgrund der gesperrten Datei wird keine der anderen Dateien eingecheckt (und keines der Prozesselemente erhält den Status "Repariert") und Benutzer A wird darüber informiert, dass keine der Dateien eingecheckt wurden, da eine der Dateien durch Benutzer B gesperrt war.

Vault Verify zum Verifizieren von Dateirevisionen

Das Vault Verify-Dienstprogramm ist eine Java-Anwendung, die Integritätsprobleme mit einem StarTeam-Native-II-Datenspeicher aufzeichnet und, falls mögliche, versucht, diese zu beheben. Es erfordert einen StarTeam-Konfigurationsnamen und, wenn sich die Datei `starteam-server-configs.xml` nicht im aktuellen Ordner befindet, den Pfadnamen des Ordners, in dem sie enthalten ist. Vault Verify öffnet die entsprechende Datenbank über JDBC, ändert die Datenbank jedoch nicht. Vault Verify analysiert zudem die Datei `hive-index.xml`, um den Speicherort der Datenspeicher-Hives zu ermitteln.

Dieses Thema enthält folgende Informationen:

- Von Vault Verify ausgeführte Prüfungen
- Vault Verify-Anforderungen
- Tipps und Empfehlungen für die Verwendung von Vault Verify

Von Vault Verify ausgeführte Prüfungen

Vault Verify ist ein Befehlszeilenprogramm, mit dem man Native-II-Datenspeicher auf beschädigte, fehlende oder verwaiste Dateien überprüfen kann. Vault Verify bietet auch die Möglichkeit, Archivdateien basierend auf den Problemen in den einzelnen Dateien zu reparieren. Dieses Dienstprogramm sucht beispielsweise verwaiste Dateien und verschiebt sie an einen angegebenen Speicherort. Der Administrator kann diese anschließend (nach dem Verifizieren der Ergebnisse) archivieren oder löschen. Die von Vault Verify ausgeführten Prüfungen werden in den folgenden Abschnitten beschrieben.

Prüfung auf beschädigte Dateien

Bei dieser Prüfung werden alle Dateien in den Archivordnern geprüft. Vault Verify stellt für alle in einem Archivordner gefundenen Dateien Folgendes sicher:

- Der Name der Archivdatei ist ein gültiger Name.
- Die Datei befindet sich basierend auf ihrem Namen im richtigen Ordner.
- Die Datei kann geöffnet und gelesen werden.
- Der MD5-Wert für die Datei entspricht ihrem Dateinamen.
- Wenn es sich um eine komprimierte (.gz) Datei handelt, ist das Format ein gültiges GZIP-Format.

Hinweis: Wenn die Option `repair` angefordert wird, werden *beschädigte* Dateien in den Standardordner oder in einen konfigurierten Ordner für *beschädigte Dateien* verschoben. Wenn die Datei verschoben wurde, wird sie als fehlend klassifiziert, wenn sie in der Datenbank referenziert wird.

Prüfung auf fehlende Dateien

Bei dieser Prüfung wird sichergestellt, dass alle in den Datenbanken definierten Archivdateien auf der Festplatte vorhanden sind. Wenn die Option `repair` angefordert wird, versucht Vault Verify, fehlende Dateien aus den Datenspeicher-Caches oder aus anderen Archivdateien wiederherzustellen.

Hinweis: Wenn Sie die Option `useca` (Cache-Agent verwenden) angeben, versucht Vault Verify, fehlende Dateien aus einem Remote-Cache-Agenten wiederherzustellen.

Prüfung auf verwaiste Dateien

Bei dieser Prüfung wird sichergestellt, dass alle im Datenspeicher enthaltenen Archivdateien durch entsprechende Datenbankdatensätze dargestellt sind. Wenn die Option `repair` angefordert wird, werden *verwaiste* Dateien in den Standardordner oder in einem konfigurierten Ordner für *verwaiste Dateien* verschoben.

Vault Verify-Anforderungen

Vault Verify erfordert Folgendes:

- Vault Verify muss Lesezugriff auf die von StarTeam-Server verwendete Datenbank haben.
- Sie müssen für Oracle-Konfigurationen den Oracle-JDBC-Treiber herunterladen und installieren. Rufen Sie die Seite http://www.oracle.com/technology/software/index.html auf, blättern Sie zum Abschnitt *Drivers* und klicken Sie auf *JDBC*. Klicken Sie auf den Link des aktuellsten JDBC-Treibers. Zum Zeitpunkt des Verfassens dieser Hilfe ist er *Oracle Database 11g* . Befolgen Sie die Download-Anweisungen. Eine Liste mit JAR-Dateien wird angezeigt. Laden Sie die .JAR-Datei herunter, die der von Ihnen verwendeten JDK-Version entspricht. **Hinweis:** Zum Herunterladen des JDBC-Treibers benötigen Sie einen Oracle.com-Benutzernamen und -Passwort. Wenn kein Konto für Sie eingerichtet ist, können Sie es auf der Anmeldeseite erstellen. Speichern Sie die JAR-Datei im Installationsordner von VaultVerify.
- Vault Verify muss Lesezugriff auf die Dateien `starteam-server-configs.xml` und `hive-index.xml` haben.
- Vault Verify benötigt Lesezugriff auf die Archivdateien der einzelnen Hives und Schreibzugriff auf die Ordner der einzelnen Hives, wenn Sie die Option `repair` verwenden.

Tipps und Empfehlungen für die Verwendung von Vault Verify

Für die Arbeit mit Vault Verify gibt es folgende Tipps und Empfehlungen:

- Sie sollten Vault Verify unter Verwendung der angepassten Batch-Datei `VaultVerify.bat` (oder der Shell-Skript-Version unter Linux) ausführen, um sicherzustellen, dass die ordnungsgemäße Java-Version verwendet wird. Die Batch-Datei (oder das Shell-Skript) befindet sich im Vault Verify-Installationsordner.
- Sie müssen das Vault Verify-Dienstprogramm auf demselben System installieren, auf dem Sie StarTeam-Server ausführen. Vault Verify wird unter dem StarTeam-Server-Installationsordner in einem eigenen Vault Verify-Ordner installiert. Auf einem Windows-System wird Vault Verify beispielsweise im Ordner `C:\Programme\Borland\StarTeam Server 2009\Vault Verify` installiert.
- Vault Verify muss Lesezugriff auf die von StarTeam-Server verwendete Datenbank haben. Es verwendet für den Zugriff auf die Datenbank standardmäßig dieselbe Benutzer-ID wie der StarTeam-Server. Wenn das Passwort für diese Benutzer-ID nicht leer ist, muss es explizit an Vault Verify übergeben werden. Es kann auch eine alternative Datenbank-Benutzer-ID übergeben werden. Beachten Sie, dass Vault Verify für Oracle-Konfigurationen unter Linux den Oracle-JDBC-Treiber benötigt, den der Kunde herunterladen und installieren muss.
- Es wird empfohlen, dass Sie Vault Verify mindestens einmal im Vierteljahr und maximal einmal im Monat ausführen. Es wird außerdem empfohlen, dass Sie Vault Verify auf einer wiederhergestellten Kopie der Produktionsdatenbank und auf das Datenspeicher-Backup (in einer Testumgebung) ausführen. Das Ausführen von Vault Verify in einer Testumgebung stellt nicht nur sicher, dass das Backup-/Wiederherstellungsverfahren funktioniert, sondern es reduziert auch die E/A-Last, die Vault Verify auf dem Produktionsserver erzeugt.
- Wenn Sie Vault Verify über eine mittelgroße bis große Datenbank laufen lassen, sollten Sie den Java-Parameter `-Xmx1024m` übergeben, damit für ausreichend Speicherplatz gesorgt ist.
- Wenn Sie die Option `corrupt` verwenden (bei dieser Prüfung werden alle Archivdateien geöffnet und gelesen) gibt Vault Verify je nach System-Hardware und Größe des Datenspeichers Ergebnisse in einem Umfang von

3 bis 30 GB/Stunde zurück. Wenn Sie zudem die Optionen `missing` und `stray` verwenden (diese Prüfungen sind viel schneller und prüfen auf das Vorhandensein von Dateien, öffnen und lesen diese jedoch nicht), kommen pro Prüfung je nach Systemhardware und Größe des Datenspeichers weitere 5 bis 30 Minuten hinzu.

- Die angeforderten Prüfoptionen werden in der folgenden Reihenfolge ausgeführt: `corrupt`, `missing` und `stray`. Wenn `repair` daher zusammen mit `corrupt` und `missing` verwendet wird, wird eine beschädigte Datei zuerst in den dafür vorgesehenen Ordner verschoben und anschließend als fehlende Datei betrachtet.
- Die angegebene StarTeam-Konfiguration kann in Gebrauch sein, wenn Vault Verify ausgeführt wird. Allerdings werden die `stray`-Überprüfung und die `repair`-Option ignoriert, wenn die StarTeam-Konfiguration in Gebrauch ist.
- Alle Ergebnisse werden einschließlich der Problemdateien im Konsolenfenster angezeigt (bei Bedarf können Sie diese Informationen in einer Textdatei speichern). Wenn Sie die Option `repair` angefordert haben, werden die Ergebnisse aller Reparaturversuche ebenfalls angezeigt. Die Option `verbose` bietet zusätzliche Fortschritts- und Diagnoseinformationen. Vault Verify verwendet eine gespeicherte Prozedur für die Angabe der Freigabe-Pfade (Projekt-/Ansichts-/Ordnerpfad) der gültigen Archivdateien, die beschädigt sind oder fehlen. Wenn dieses Verfahren nicht vorhanden ist, wird nur der Name der Problemdateien angegeben, die Freigabe-Pfade jedoch nicht.
- Das Vault Verify-Dienstprogramm ist in mehreren JAR-Dateien enthalten. Die Hauptdatei is `VaultVerify.jar`. Sie erfordert JRE 1.5 oder höher. Um Hilfe zu Vault Verify zu erhalten, können Sie `java -jar VaultVerify.jar -help` eingeben. In diesem Hilfesystem finden sich auch Hinweise zur Verwendung des Programms. Weitere Informationen zu den Vault Verify-Befehlszeilenoptionen finden Sie unter dem Link "Referenz" am Ende dieses Themas.
- StarTeam-Server sucht immer in seinem eigenen Installationsordner nach der Datei `starteam-server-config.xml`, um zu ermitteln, ob der Server ausgeführt wird. Bedenken Sie diese Tatsache, wenn Sie diese Datei an einen anderen Speicherort kopieren und anschließend in Vault Verify den neuen Speicherort mit der Option `path` angeben. Wenn Sie in der kopierten Version der Datei `starteam-server-config.xml` angegeben haben, dass der Server nicht ausgeführt wird, und die Optionen `stray` und `repair` in Vault Verify verwenden, werden diese Optionen nicht ignoriert, wenn der StarTeam-Server ausgeführt wird.
- Bei dem an Vault Verify übergebenen Namen der Serverkonfiguration muss die Groß-/Kleinschreibung beachtet werden. Wenn der Name Leerzeichen enthält, müssen Sie den an Vault Verify übergebenen Konfigurationsnamen in Anführungszeichen setzen.
- Vault Verify verwendet standardmäßig für den Zugriff auf die Datenbank dieselbe Benutzer-ID wie der StarTeam-Server. Wenn das Passwort für diese Benutzer-ID nicht leer ist, muss es explizit an Vault Verify übergeben werden. Es kann auch eine alternative Datenbank-Benutzer-ID übergeben werden.
- Die Ausgabe von Vault Verify wird standardmäßig im Befehlsfenster angezeigt. Borland empfiehlt, die Ausgabe in eine Datei umzuleiten, sodass Sie, falls erforderlich, die Informationen an den technischen Support von Borland senden können.

Verwandte Verfahrensweisen

Dateirevisionen mit Vault Verify verifizieren

Daten von Auscheckvorgängen mit dem Checkout Trace-Dienstprogramm untersuchen

Das Checkout Trace-Dienstprogramm von StarTeam generiert eine `*.csv`-Datei, die Daten zu Auscheckvorgängen für die Serverkonfiguration enthält, für die die Ablaufverfolgung aktiviert ist. Bevor Sie das Dienstprogramm ausführen können, müssen Sie die Ablaufverfolgung für die Serverkonfiguration in der Datei `starteam-server-configs.xml` aktivieren. Bei aktivierter Ablaufverfolgung generiert der Server für jede ausgecheckte Datei einen Trace-Datensatz und speichert die Informationen in einer Trace-Datei (`check-out.cotrc`). Das Dienstprogramm verwendet die Trace-Datei als Input und liefert eine `*.csv`-Datei mit Daten zu den Auscheckvorgängen. Sie können die Ausgabe aus der `*.csv`-Datei in Datamart oder in ein Excel-Arbeitsblatt importieren.

Die `*.csv`-Datei enthält für alle Auscheck-Vorgänge folgende Informationen:

Hinweis: In der generierten `.cotrc`-Datei sind keine Auscheckdaten enthalten, wenn das Auschecken von einem Cache-Agenten vorgenommen wurde. Es sind nur dann Daten in der `.cotrc`-Datei enthalten, wenn der Auscheckvorgang vom Server vorgenommen wurde.

- Benutzer-ID
- Benutzername
- Zeitstempel (Datum/Uhrzeit des Auscheck-Vorgangs)
- Projekt-ID
- Projekt
- Ansicht
- Ansichts-ID
- Ordner-ID
- Ordnerpfad
- Datei-ID
- Dateiname
- Revisionsnummer der Datei

Hinweis: Um die Leistung zu optimieren, aktualisiert StarTeam Trace-Dateien nicht sofort. StarTeam puffert die Informationen für die Trace-Datei im Speicher und schreibt sie zu Zeiten geringer Speicherauslastung in die Trace-Datei.

Sie finden das Checkout Trace-Dienstprogramm im Stammorder der StarTeam-Server-Installation (`CheckoutTraceDump.exe`). Weitere Informationen zur Verwendung dieses Dienstprogramms finden Sie unter den Links am Ende dieses Themas.

Verwandte Verfahrensweisen

Daten aus Auscheckvorgängen verfolgen

Sicherheitsprotokolle

Die Anwendungs-Clients und -Server erzeugen eine Reihe von Protokolldateien. Mithilfe dieser Protokolle können Administratoren die Leistung des Systems beurteilen und den Ursachen von Problemen möglicherweise auf den Grund gehen. Jede Serverkonfiguration verfügt über ein eigenes Serverprotokoll und ein Sicherheitsprotokoll. Jeder Client erzeugt seine eigene Protokolldatei, in der die Aktivitäten zwischen dem Client und der mit dem Client verbundenen Serverkonfiguration aufgezeichnet werden.

Benutzer müssen über entsprechende Sicherheitszugriffsrechte verfügen, um Protokolldateien anzeigen zu können. Diese Zugriffsrechte können über die Menüoption **Tools ▸ Konten ▸ Zugriffsrechte** im **Serveradministrations-Tool** festgelegt werden. Weitere Informationen zu Zugriffsrechten finden Sie unter "Zugriffsrechte und Berechtigungen" im Abschnitt "Verwandte Informationen" weiter unten.

In den nachstehenden Abschnitten wird Folgendes beschrieben:

- Serverprotokolldateien
- Sicherheitsprotokolldateien
- Client-Protokolldatei (`StarTeam.Log`)

Serverprotokolldateien

In der Serverprotokolldatei (`Server.Länderkennung`) werden die Aktivitäten einer Serverkonfiguration aufgezeichnet. Bei jedem Start einer Serverkonfiguration benennt der Server die bestehende Protokolldatei um und erstellt eine neue Protokolldatei für die aktuelle Sitzung der Serverkonfiguration. Die Protokolldatei des vorhergehenden Starts der Konfiguration erhält einen Namen, der das Datum und die Uhrzeit des Zeitpunkts erhält, zu dem die Datei umbenannt wurde (`Server.Länderkennung.Datum.Log`). Wenn Sie beispielsweise eine Serverkonfiguration am 9. November 2005 um 17:22 Uhr starten, wird die alte Datei `Server.Länderkennung.Log` in `Server.de-De.2005-11- 09-17-22-59.Log` umbenannt und es wird eine neue Datei `Server.Länderkennung.Log` erstellt, deren Zeitstempel `11/9/2005 17:23:03` lautet.

Wenn die Ländereinstellung des Betriebssystems, auf dem der Server ausgeführt wird, nicht "en-US" ist, werden zwei Serverprotokolldateien erstellt: eine für US-Englisch und eine für Ihre Ländereinstellung. Sie könnten beispielsweise die Dateien `Server.en-US.Log` und `Server.de-De.Log` haben. Das erste Protokoll wird für Unterstützungszwecke benötigt und das zweite kann von Ihnen verwendet werden.

Sie können den Inhalt der Serverprotokolldatei anzeigen, auch, während die Serverkonfiguration ausgeführt wird, indem Sie **Tools ▸ Administration ▸ Serverprotokoll** wählen. Nur die letzten 64 KB der Protokolldateidaten werden angezeigt. Die gesamte Datei kann im Windows-Editor, in WordPad oder in einem anderen Texteditor angezeigt werden.

Sicherheitsprotokolldateien

In einem Sicherheitsprotokoll werden alle sicherheitsrelevanten Ereignisse für eine Serverkonfiguration aufgezeichnet. Das Protokoll enthält eine Auflistung aller sicheren Ereignisse (z. B. das An- oder Abmelden), Datums- und Zeitangaben der Ereignisse, die ausführenden Benutzer der Operationen, die Workstations, auf denen die Operationen ausgeführt wurden, die Elemente, für die die Aktionen ausgeführt wurden, und Informationen darüber, ob die Operationen fehlgeschlagen sind.

Abhängig von der Anzahl der Benutzer und dem Umfang der Aktivitäten in einer Serverkonfiguration kann das Sicherheitsprotokoll sehr schnell anwachsen. Der Server kann alte Einträge löschen, um die Größe des Protokolls auf ein vernünftiges Maß zu beschränken. Entscheiden Sie zunächst, wie lange Sicherheitsereignisse gespeichert werden sollen, und legen Sie anschließend in der Serverkonfiguration fest, dass ältere Einträge gelöscht werden. Weitere Informationen zum Bereinigen von Einträgen im Sicherheitsprotokoll finden Sie unter dem Thema "Mit dem Sicherheitsprotokoll arbeiten" im Abschnitt "Verwandte Informationen".

Wenn Sie über Zugriffsrechte für eine Serverkonfiguration verfügen, können Sie das entsprechende Sicherheitsprotokoll jederzeit anzeigen. Das Sicherheitsprotokoll ist keine gewöhnliche .Log-Datei, da die Daten des Protokolls in der Anwendungsdatenbank gespeichert werden. Das Sicherheitsprotokoll ist über das Menü **Tools** ▸ **Konten** ▸ **Sicherheitsprotokoll** verfügbar.

StarTeam-Protokolldatei

In der Datei `StarTeam.Log` werden alle Operationen protokolliert, die auf Ihrer Client-Workstation während einer Sitzung durchgeführt wurden. Die Datei dokumentiert Fehler und fehlgeschlagene Operationen zwischen dem Server und Ihrer Workstation während Serverkonfigurationssitzungen, sodass die Ursachen der Fehler leichter erkannt werden können.

Die Datei "StarTeam.Log" kann folgende Arten von Informationen enthalten:

- Befehle, die von Ihrer Workstation an eine Serverkonfiguration gesendet werden, wenn Sie ein Projekt öffnen und damit arbeiten. Wenn Sie mit Projekten aus unterschiedlichen Serverkonfigurationen arbeiten, können Sie die Datei `StarTeam.Log` so konfigurieren, dass der Name der Serverkonfiguration gemeinsam mit den Befehlsinformationen aufgezeichnet wird.
- Befehle, die lokal auf Ihrer Workstation ausgeführt werden, z. B. das Festlegen von persönlichen Optionen.
- Fehlermeldungen, die bei der Verwendung der Anwendung aufgezeichnet werden.
- Ereignisse, die von StarTeamMPX ausgeführt werden.

Die Datei 'StarTeam.Log' erstellen

Jedes Mal, wenn Sie Ihren Client starten, erstellt das System eine `StarTeam.Log`-Datei in dem Ordner, den Sie in Ihren persönlichen Optionen angegeben haben.

Speicherort der StarTeam.Log-Datei

Auf den meisten Systemen ist der Standardspeicherort für die `StarTeam.Log`-Datei `C:\Programme\Borland \StarTeam x.x`. Wenn in dem Ordner bereits eine Datei namens `StarTeam.Log` vorhanden ist, benennt die Anwendung die vorhandene Datei um und fügt das Datum und die Uhrzeit der Umbenennung zum Dateinamen hinzu. Wenn Sie beispielsweise am 1. Juli 2009 um 10.35 Uhr eine `StarTeam.Log`-Datei erstellen, wird die alte `StarTeam.Log`-Datei in `StarTeam-09-Nov-05-10-35-18.Log` umbenannt und es wird eine neue `StarTeam.Log`-Datei erstellt.

Tipp: Tipp: Da die Anwendung bei jedem Start des Clients eine neue `StarTeam.Log`-Datei erstellt, wächst die Größe des Ordners für die StarTeam-Protokolldatei möglicherweise sehr schnell an. Um die Anzahl der Protokolldateien in dem Ordner zu steuern, sollten Sie regelmäßig alte Protokolldateien aus dem Ausgabeordner löschen oder die `StarTeam.Log`-Option deaktivieren. Um diese Option zu deaktivieren, heben Sie die Markierungen der Auswahlfelder für **Protokollfehler** und **Protokolloperationen** im Register **Arbeitsbereich** des Dialogfelds **Persönliche Optionen** auf.

Verwandte Verfahrensweisen

Mit dem Serverprotokoll arbeiten
Mit dem Sicherheitsereignisprotokoll arbeiten
'StarTeam.Log' anzeigen und anpassen

Verwandte Referenz

Zugriffsrechte und Berechtigungen
Sicherheitsereignistypen

Übersicht über Initialisierungsdateien

Initialisierungsdateien werden bei den unterschiedlichen Windows-Plattformen an unterschiedlichen Speicherorten abgelegt. Unter NT ist der *Pfad-Präfix* `C:\interoffice`. Unter 2000 und XP ist der *Pfad-Präfix* `C:\Dokumente und Einstellungen`.

Des Weiteren werden in diesem Thema die unterschiedlichen Initialisierungsdateien beschrieben, die von StarTeam verwendet werden.

ConnectionManager.ini

Die Datei `ConnectionManager.ini` enthält Informationen, die der Anwendungs-Client für die Ausführung benötigt. Sie wird bei der Installation der Anwendung erstellt.

Bei den unten aufgeführten Daten handelt es sich nur um Beispieldaten. 'x' wird durch eine hexadezimale Zahl ersetzt.

```
[ConnectionManager] WorkstationID=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

starteam-server-configs.xml

Die Datei `starteam-server-configs.xml` enthält Sitzungsoptionen für eine oder mehrere Serverkonfigurationen. In den Serversitzungsoptionen werden die Hauptinformationen gespeichert, die der Server benötigt, um eine Serverkonfiguration zu starten. Für jeden Computer existiert eine `starteam-server-configs.xml`-Datei, die jeweils im gleichen Ordner wie die Serveranwendung gespeichert wird. Unter Windows wird die Datei in der Regel unter `C:\Programme\Borland\StarTeam Server` gespeichert.

Die Sitzungsoptionsdaten jeder Serverkonfiguration beginnen mit dem Namen der Konfiguration in Klammern, gefolgt von Optionen und den zugehörigen Einstellungen. Der Server erstellt und verwaltet diese Datei, die beim Erstellen der ersten Serverkonfiguration erzeugt wird. Die Datei wird aktualisiert, wenn eine Serverkonfiguration erstellt, geändert, gelöscht, gestartet oder gestoppt wird. Bearbeiten Sie die Datei nicht direkt.

Borland empfiehlt, eine Sicherungskopie der Datei `starteam-server-configs.xml` anzulegen oder die Datei der Versionskontrolle zu unterstellen.

Tipp: Weitere Informationen sowie eine Beschreibung der in dieser Datei enthaltenenen Informationen finden Sie unter dem Link "starteam-server-configs.xml" am Ende dieses Themas.

starteam-client-options.xml

Die Datei `starteam-client-options.xml` enthält eine Zeile für jede Option, die im Dialogfeld **Persönliche Optionen** festgelegt werden kann (Sie können das Dialogfeld öffnen, indem Sie **Tools** ▸ **Persönliche Optionen**) im Hauptmenü des Cross-Platform Client wählen). Die meisten Optionsbezeichnungen in der Datei `starteam-client-options.xml` sind den englischen Bezeichnungen der entsprechenden Optionen in dem Dialogfeld sehr ähnlich. Für alle Optionen, die im Dialogfeld "Persönliche Optionen" über Auswahlfelder verfügen, wird der Wert `1` für "aktiviert" und der Wert `0` für "deaktiviert" vergeben. Je nach Option werden Intervalle auf eine Anzahl von Minuten oder Sekunden festgelegt. Pfade werden als Text angegeben. Im Text werden keine Anführungszeichen verwendet.

Beispielsweise enthält der Eintrag "Project Component" die Pfadangaben der alternativen Arbeitsordner für Projekte, auf die von Ihrer Workstation aus zugegriffen wird. Der Eintrag für diese Komponente in der `starteam-client-options.xml`-Datei besteht aus folgenden Teilen:

- Den Wörtern *Project Component*.

- *ViewWorkingFolderOverrides* (Angabe eines alternativen Arbeitsordners für eine komplette Ansicht) oder *WorkingFolderOverrides* (Angabe eines alternativen Arbeitsordners für einen einzelnen Ordner).
- Einer hexadezimalen Darstellung der Projektansicht und des Projektordners.
- Dem alternativen Pfad für den Arbeitsordner.

starteam-servers.xml

In der Datei `starteam-servers.xml` werden die Serverkonfigurationen gespeichert, für die Sie Serverbeschreibungen eingegeben haben, welche beim Öffnen und Erstellen von Projekten verwendet werden. Auf einem Windows XP-System befindet sich diese Datei z. B. im Ordner `C:\Dokumente und Einstellungen\<Benutzer>\Application Data\Borland\StarTeam`.

Die Initialisierungsdateien werden auf den unterschiedlichen Windows-Plattformen an unterschiedlichen Speicherorten abgelegt. Unter NT lautet der *Pfad-Präfix* `C:\winnt\Profiles`. Unter 2000 und XP ist der *Pfad-Präfix* `C:\Dokumente und Einstellungen`.

Sowohl unter UNIX als auch unter Windows kann der Standard-Speicherort der Datei `starteam-servers.xml` geändert werden, indem

```
-f NeueServerListenDatei
```

zum Java-Befehl der Batch/Skript-Datei `serveradmin` hinzugefügt wird. Der neue Dateiname und der neue Speicherort werden im Feld `starteam-servers.xml` im Serveradministrations-Tool angezeigt.

Jedes Mal, wenn Sie eine Serverkonfiguration auf dem Client oder im Serveradministrations-Tool aktualisieren oder hinzufügen, wird diese Datei aktualisiert.

Verwandte Verfahrensweisen

Protokoll- und Initialisierungsdateien verwalten

Verwandte Referenz

Referenzen für Initialisierungsdateien
starteam-server-configs.xml

Testserver verwenden

Eine einfache, jedoch häufig übersehene Maßnahme zum Optimieren administrativer Vorgänge in Ihrer Umgebung ist die Bereitstellung einer StarTeam-Server-Konfiguration als Testserver. Ihr Testserver kann kostengünstigere Hardware als Ihr Produktionsserver verwenden, sollte aber auf einer Backup-Kopie des Produktionsservers ausgeführt werden können. Mit dieser Möglichkeit kann der Testserver viele nützliche Vorteile bieten:

- Sie können neue SDK-Anwendungen, Workflow-Regeln, Release-Verfahren usw. auf dem Testserver testen, ohne Angst haben zu müssen, dass dies zu unerwünschten Auswirkungen auf dem Produktionsserver führt.
- Sie können den Testserver verwenden, um neue Versionen von StarTeam bereitzustellen und um Aktualisierungs- und Migrationsvorgänge zu simulieren, bevor Sie sie auf dem Produktionsserver anwenden.
- Sie können den Testserver für Schulungszwecke für neue Entwickler und Administratoren verwenden.
- Sie können Backup- und Wiederherstellungsverfahren für Ihre Organisation testen. Sobald Sie sichergestellt haben, dass die Notfallverfahren funktionieren, können Sie den Testserver bei einem Ausfall des Produktionsservers als Backup-Computer verwenden.

Hinweis: Ab StarTeam Server 2009 erstellt der Server neue Projekte, bei denen nur der Typ "Datei" als Vorgabe für neue Ansichten vorab ausgewählt ist. Benutzer können die Projekteigenschaften nach wie vor nach Erstellen des Projekts ändern und sie können auch die aufgenommenen Elementtypen für eine neue Ansicht ändern. Wenn allerdings der Benutzer nichts ändert, enthalten neue Ansichten nur dann standardmäßig Dateien, wenn sie erstellt werden.

Diese Änderung wirkt sich nicht auf vorhandene Projekte aus. Sie betrifft nur neue Projekte, die mit StarTeam Server 2009 oder vorhandenen Servern, die auf StarTeam Server 2009 aktualisiert wurden, erstellt wurden. Durch das Hinzufügen von anderen Elementtypen zu den Projekteigenschaften (nachdem die Ansicht erstellt wurde) wird die Ansicht NICHT mit den Elementen gefüllt, die in der übergeordneten Ansicht enthalten waren (aber während des Erstellens der neuen Ansicht übergangen wurden). Falls der Benutzer die vorherigen Elemente in die neue Ansicht aufnehmen möchte, muss er sie abrufen, indem er die Basis von der übergeordneten Ansicht ändert.

Verwandte Verfahrensweisen

Informationen sichern

Backups

Dieser Abschnitt enthält konzeptionelle Themen, die sich mit dem Erstellen von Backups befassen.

In diesem Abschnitt

Zu sichernde Komponenten

Dieses Thema beschreibt, von welchen StarTeam-Dateien ein Backup erstellt werden muss.

Wenn Sie ein Backup von StarTeam erstellen, müssen Sie die folgenden Ordner und Dateien sichern:

- Die Datei `starteam-server-configs.xml`. Diese Datei enthält die Serverkonfigurationen. Sie befindet sich im Installationsordner des Servers.
- Die Datenbankdateien. Jede Serverkonfiguration hat eine Datenbank (bzw. einen Schema-Benutzer bei Oracle).
- Den Ordner *Attachments*und seine untergeordneten Ordner. Diese Ordner enthalten die an Änderungsanforderungen, Tasks, Themen usw. angehängten Dateien.
- Den Ordner *HiveIndex*.
- Den Ordner *Archive* für jeden einzelnen Hive. Beachten Sie, dass es nicht erforderlich ist, den Ordner *Cache* für jeden der einzelnen Hive zu sichern.

Alle diese Dateien sollten zur gleichen Zeit und, wenn möglich, auf demselben Band gesichert werden.

Tipp: Weitere Informationen zu Backups finden Sie unter dem Link "StarTeam-Backups" am Ende dieses Themas.

Verwandte Konzepte

Native-II-Datenspeicher und Hives
StarTeam Backups
Übersicht über die Datenspeicherung

Verwandte Verfahrensweisen

Neue Hives erstellen
Optionen für die Datenspeicherung konfigurieren

StarTeam Backups

Da StarTeam Native-II-Datenspeicher verwendet, können Sie Backups vollständig online ausführen, ohne die Server sperren zu müssen. Mit dem StarTeam-Native-II-Datenspeicher können Sie mehrere Hives erstellen, von denen jeder seinen eigenen Archivbereich enthält, der gesichert werden muss. Sie können Hives dynamisch hinzufügen, um die Adressierbarkeit des Datenspeichers zu erhöhen. Sie müssen dabei jedoch sicherstellen, dass Sie den Backup-Prozess entsprechend aktualisieren.

Tipp: Weitere Informationen zu Native-II-Datenspeichern und Hives finden Sie in den Links "Übersicht über die Datenspeicherung" und "Native-II-Datenspeicher und Hives" am Ende dieses Themas.

Des Weiteren wird ein Online-Backup-Verfahren und ein dazugehöriger Wiederherstellungsplan beschrieben.

Online-Backups

Das Online-Backup-Verfahren, das die Merkmale des Native-II-Datenspeichers nutzt, ist im Folgenden zusammengefasst:

1. Sichern Sie die Datenbank unter Verwendung des Online-Backup-Verfahrens für Datenbanken.
2. Wenn das Datenbank-Backup abgeschlossen ist, erstellen Sie ein Online-Backup der Anhangs- und Archivordner der einzelnen Hives. Diese Backups können gleichzeitig ausgeführt werden. Zudem kann ein Zeitplan für vollständige/inkrementelle Backups verwendet werden, sodass vollständige Backups beispielsweise wöchentlich und inkrementelle Backups täglich ausgeführt werden.
3. Erstellen Sie ein Backup des Ordners "HiveIndex" für das Repository.
4. Erstellen Sie ein Backup der Datei `starteam-server-configs.xml`.

Hinweis: Der Server ist niemals gesperrt. Deshalb bleibt die vollständige Funktionalität immer verfügbar.

Wiederherstellungsplan

Beachten Sie, dass das Backup des Datenspeichers (Anhänge und Archiv) in diesem Schema chronologisch vor den Informationen im Datenbank-Backup liegen. Dies bedeutet, dass die Archiv- und Anhangsordner neuere Dateien enthalten können, die in der gesicherten Datenbank nicht enthalten sind. Dies stellt kein Problem dar, da das Wiederherstellungsverfahren hinsichtlich Zeitdiskrepanzen tolerant ist.

Im Folgenden finden Sie einen Wiederherstellungsplan, der dem in letzten Abschnitt zusammengefassten Online-Backup-Plan entspricht:

1. Laden Sie die Datenbank aus dem letzten Backup neu.
2. Laden Sie gleichzeitig die Archiv- und Anhangsordner aus dem letzten Backup. Wenn Sie die vollständigen und inkrementellen Backups verwendet haben, können Sie das letzte vollständige Backup und gleichzeitig alle nachfolgenden inkrementellen Backups neu laden.

Wenn Sie alles neu geladen haben, kann das Repository verwendet werden. Es stellt kein Problem dar, wenn die Archiv- oder Anhangsordner Dateien neueren Datums enthalten, die in der Datenbank nicht enthalten sind. StarTeam ignoriert die Dateien neueren Datums und wenn diese Dateirevisionen später hinzugefügt werden, überschreibt StarTeam die vorhandenen Dateien.

Verwandte Konzepte

- Native-II-Datenspeicher und Hives
- Übersicht über die Datenspeicherung

Verwandte Verfahrensweisen

- Neue Hives erstellen
- Optionen für die Datenspeicherung konfigurieren

Übersicht über das Verschieben von Serverkonfigurationen

Bevor Sie versuchen, eine Serverkonfiguration zu verschieben, sollten Sie von allen StarTeam-Komponenten ein Backup erstellen:

- Datenbank
- Repository
- Datei `starteam-server-configs.xml`

Tipp: Weitere Informationen zu den zu sichernden Dateien finden Sie unter dem Link "Zu sichernde Komponenten" am Ende dieses Themas.

Des Weiteren bietet dieses Thema eine Übersicht über das Verschieben von Serverkonfigurationen und einige falsche Annahmen, die beim Verschieben von Serverkonfigurationen zu Fehlern führen können.

Übersicht über das Verschieben einer Serverkonfiguration

Im Folgenden finden Sie eine datenbankunabhängige Übersicht über das Verschieben einer Serverkonfiguration:

1. Fahren Sie die Serverkonfiguration herunter. Da Sie Native-II-Datenspeicher verwenden, ist dies nicht wirklich erforderlich, es wird dennoch empfohlen.
2. Erstellen Sie ein Backup der Datenbank.
3. Überprüfen Sie den Speicherort der zu verschiebenden Dateien. Diese sind das Datenbank-Backup, die Datei `starteam-server-configs.xml` sowie das Repository einschließlich der Native-II-Archive, sofern diese nicht im Repository enthalten sind.
4. Kopieren Sie die Dateien vom Quell- an den Zielspeicherort.
5. Kopieren Sie den **Eintrag** für die Quell-Serverkonfiguration in die Zieldatei `starteam-server-configs-xml` . Wenn diese Datei auf dem Zielcomputer nicht vorhanden ist, kopieren Sie die gesamte Datei und löschen Sie alle Einträge aus der Datei für Serverkonfigurationen, die auf dem Zielcomputer nicht vorhanden sind. Wenn diese Datei auf dem Zielcomputer vorhanden ist, achten Sie darauf, dass Sie nur den Abschnitt kopieren, der für die Serverkonfiguration erforderlich ist, die Sie auf den Zielcomputer verschieben.
6. Korrigieren Sie den Repository-/Protokollpfad in der Datei `starteam-server-configs.xml` für die angegebene Serverkonfiguration.
7. Stellen Sie die Datenbank aus dem Backup wieder her.
8. Konfigurieren Sie eine ODBC-Verbindung.
9. Falls erforderlich, starten Sie die Serverkonfiguration mit der Option **Mit angepassten Serveroptionen starten** neu. Weitere Informationen hierzu finden Sie unter dem Link "Serverkonfigurationen starten und stoppen" am Ende dieses Themas.

Falsche Annahmen zum Verschieben von Serverkonfigurationen

Im Folgenden finden Sie einige falsche Annahmen zum Verschieben von Serverkonfigurationen, die zu Fehlern führen können. Sie sollten die folgenden Methoden daher nicht ausprobieren:

- Verschieben Sie die Datenbank einfach und erstellen Sie eine neue Serverkonfiguration, die auf sie verweist.
- Die Serverkonfiguration besteht nur aus einer Datenbank und einem Repository. Beachten Sie, dass die Datei `starteam-server-configs.xml` beim Verschieben einer Serverkonfiguration ebenfalls erforderlich ist.

- Verwenden Sie einfach den Symbolleistenschalter **Datenbank migrieren**. Beachten Sie, dass diese Option nur Datenbanken migriert.

Hinweis: Wenn Sie beim Migrieren einer Serverkonfiguration Hilfe benötigen, wenden Sie sich an den Borland StarTeam Support unter http://support.borland.com .

Verwandte Konzepte

Native-II-Datenspeicher und Hives
Übersicht über die Datenspeicherung
StarTeam Backups
Zu sichernde Komponenten

Verwandte Verfahrensweisen

Serverkonfigurationen starten und stoppen
Serverkonfigurationen auf einen neuen Server verschieben

Online-Backups

Wenn alle Archivdateien einer Serverkonfiguration im Native-II-Format abgelegt sind, können Sie die Konfiguration online sichern, ohne diese hierfür herunterfahren oder sperren zu müssen. Außerdem muss die Datenbank für Online-Backups eingerichtet werden. Weitere Informationen zu Datenbank-Backups finden Sie unter dem Link "Datenbank-Backups" am Ende dieses Themas.

Der Datenspeicher sollte immer erst nach Abschluss des Datenbank-Backups gesichert werden. Die beiden Backups sollten nie gleichzeitig durchgeführt werden. So stellen Sie sicher, dass alle in der Datenbank referenzierten Komponenten den richtigen Speicherort im Datenspeicher zugewiesen bekommen. Dateien, die der Datenbank nicht bekannt sind, verursachen keine Probleme.

Die Ordner *HiveIndex.xml* und *Attachments* sollten neben den Archivordnern des jeweiligen Hives im Datenspeicher-Backup enthalten sein. Die Sicherung des Cache-Ordners der Hives ist optional. In der Regel befinden sich die Datenbank und der Datenspeicher auf unterschiedlichen Computern. Der Datenspeicher selbst kann auf mehrere Volumes und auf unterschiedliche Computer verteilt sein. Weitere Informationen zu den zu sichernden Daten finden Sie unter dem Link "Zu sichernde Komponenten" am Ende dieses Themas.

Falls

- die Datenbank verloren geht sollte, muss der Administrator das letzte vollständige Backup der Datenbank wiederherstellen und mithilfe der Redo-Logs (Oracle) oder inkrementeller Backups (MS SQL Server) ein Rollforward der Datenbank auf die Datenspeicherzeit vornehmen.
- der Datenspeicher verloren gehen sollte, muss ein Backup der Datenbank in ihrem aktuellen Zustand einschließlich der Transaktionsprotokolle (Redo-Logs) durchgeführt werden, bevor man mit der Wiederherstellung beginnen kann.
- der Datenspeicher verloren geht (oder Datenspeicher und Datenbank), muss der Serveradministrator sowohl die Datenbank als auch den Datenspeicher über das letzte vollständige Backup wiederherstellen. Nachdem das Online-Datenbank-Backup wiederhergestellt wurde, muss ein Rollforward der Datenbank auf den Backup-Zeitpunkt des Datenspeichers erfolgen.

Hinweis: Ein Fehlen von Transaktionsprotokollen (Redo-Logs) kann zu Datenverlust führen und die Wiederherstellungsmöglichkeiten im Notfall einschränken.

Verwandte Konzepte

Native-II-Datenspeicher und Hives
StarTeam Backups
Übersicht über die Datenspeicherung
Zu sichernde Komponenten
Datenbank-Backups

Verwandte Verfahrensweisen

Neue Hives erstellen
Optionen für die Datenspeicherung konfigurieren

Datenbank-Backups

Dieser Abschnitt enthält konzeptionelle Themen, die sich mit dem Erstellen von Datenbank-Backups befassen.

In diesem Abschnitt

Übersicht über Datenbank-Backups

In diesem Abschnitt werden die Backup-Optionen vorgestellt, die Datenbankadministratoren zur Verfügung stehen. Außerdem enthält es Empfehlungen für die Sicherung der Datenbanken, die von Serverkonfigurationen verwendet werden. Beachten Sie, dass es sich hierbei wirklich nur um Empfehlungen handelt. Endgültige Pläne für eine Wiederherstellung im Notfall müssen in Ihrem Unternehmen gemeinsam mit den für die IT-Infrastruktur zuständigen Mitarbeitern erstellt werden.

Hinweis: Ein Backup setzt sich aus einer Sicherung der Datenbank und der Archivdateien der Anwendung zusammen. Weitere Informationen zu den zu sichernden Daten finden Sie unter dem Link "Backups" am Ende dieses Themas.

Verwandte Konzepte

Zu sichernde Komponenten
Native-II-Datenspeicher und Hives
StarTeam Backups
Übersicht über die Datenspeicherung
Backups von Oracle-Datenbanken
Backups von SQL Server-Datenbanken
Backups

Verwandte Verfahrensweisen

Neue Hives erstellen
Optionen für die Datenspeicherung konfigurieren

Backups von SQL Server-Datenbanken

Bei der Online-Sicherung von Serverkonfigurationen ist es sehr wichtig, vollständige Backups der Datenbank- und der Transaktionsprotokolle zu erstellen. Des Weiteren wird in diesem Thema beschrieben, welche Backup-Typen von SQL Server unterstützt werden, und es enthält Empfehlungen zum Ausführen von SQL Server-Backups.

SQL Server-Backup-Typen und -Wiederherstellungsmodelle

SQL Server 2005 unterstützt die folgenden Backup-Typen:

Vollständiges Datenbank-Backup	Vollständige Datenbank-Backups enthalten eine vollständige Kopie des Datenbankzustands zu dem Zeitpunkt, zu dem der Backup-Vorgang initiiert wurde. Sie enthalten ein Abbild der aktuellen Daten der Datenbank. Für die meisten Wiederherstellungsoptionen wird ein vollständiges Backup benötigt.
Differenz-Backup	Bei einem Differenz-Backup werden nur die Daten gesichert, die seit dem letzten vollständigen Datenbank-Backup geändert wurden. Es empfiehlt sich, regelmäßige Differenz-Backups zu planen, da diese kleiner sind und schneller erstellt werden können. Differenz-Backups ohne vorhergehende vollständige Backups sind jedoch nutzlos.
Backup des Transaktionsprotokolls	Bei einem Backup des Transaktionsprotokolls werden alle Transaktionen erfasst, die seit dem letzten Backup des Transaktionsprotokolls durchgeführt wurden. Backups des Transaktionsprotokolls ermöglichen die Wiederherstellung bis zur letzten festgeschriebenen Transaktion.
Datei- oder Dateigruppen-Backup	Bei einem Datei- oder Dateigruppen-Backup werden einzelne Dateien (oder die Dateien einer Dateigruppe) gesichert. Die Dateien einer Datenbank können einzeln gesichert und wiederhergestellt werden.

Durch Wiederherstellen der Datenbank wird diese in einem einzelnen Schritt aus einem Datenbank-Backup neu erstellt. Beim Wiederherstellungsvorgang wird die vorhandene Datenbank überschrieben oder eine Datenbank neu erstellt, wenn noch keine vorhanden ist. Die wiederhergestellte Datenbank entspricht dem Zustand, den die Datenbank zum Zeitpunkt der Fertigstellung des Backups hatte - abzüglich aller nicht zurückgeschriebenen Transaktionen. Nicht zurückgeschriebene Transaktionen werden zurückgesetzt ("Rollback"), wenn die Datenbank wiederhergestellt wird.

Der Datenbankadministrator kann das Wiederherstellungsmodell für die Datenbank abhängig von den Ressourcenanforderungen wählen. Das Wiederherstellungsmodell sollte ein Kompromiss sein zwischen Protokollierungs-Overhead einerseits und Wichtigkeit der vollständigen Datenwiederherstellung andererseits.

Folgende Wiederherstellungsmodelle werden von SQL Server 2005 SP2 unterstützt:

Vollständig	Die Daten sind kritisch und der Zustand zum Zeitpunkt des Fehlers muss wiederhergestellt werden können. Alle Datenänderungen werden protokolliert. Alle SQL Server 2005 SP2-Wiederherstellungsoptionen sind verfügbar.
Bulk-Protokollierung	Einige Bulk-Operationen, z. B. Bulk-Kopiervorgänge, SELECT INTO und Textverarbeitung können bei Bedarf erneut eingespielt werden, sodass diese Operationen nicht vollständig protokolliert werden müssen. Es kann nur der Zustand des letzten Datenbank- oder Protokoll-Backups wiederhergestellt werden.
Einfach	Alle nach dem letzten Backup vorgenommenen Datenänderungen sind nicht mehr verfügbar. Bei dieser Art von Wiederherstellung wird der geringste Prokollierungs-Overhead erzeugt, aber nach dem letzten Backup vorgenommene Änderungen können nicht wiederhergestellt werden.

Zur Wiederherstellung des Datenbankzustands zu einem bestimmten Zeitpunkt (beispielsweise bevor unerwünschte Daten eingegeben wurden) muss entweder das Wiederherstellungsmodell "Vollständig" oder "Bulk-Protokollierung" verwendet werden.

Vollständige Backups von SQL Server-Datenbanken

Bei einem vollständigen Datenbank-Backup wird ein Duplikat der Daten in der Datenbank erstellt. Dabei handelt es sich um einen einzelnen Vorgang, der üblicherweise in regelmäßigen Abständen ausgeführt wird. Vollständige Datenbank-Backups sind in sich abgeschlossen. Sie enthalten ein Abbild der aktuellen Daten der Datenbank. Für die meisten Wiederherstellungsoptionen wird ein vollständiges Backup benötigt.

Borland rät zur Erstellung vollständiger Backups.

Differenzielle Backups von SQL Server-Datenbanken

Bei differenziellen Backups werden nur die Daten gesichert, die seit dem letzten Datenbank-Backup geändert wurden. Zur Reduzierung der für die Sicherung benötigten Zeit werden regelmäßige Differenz-Backups empfohlen. Die häufige Erstellung von Backups vermindert das Risiko eines Datenverlusts.

Differenz-Backups ermöglichen die Wiederherstellung der im Backup enthaltenen Daten in der Datenbank. Mithilfe von Differenz-Backups kann der Zustand der Datenbank zu einem bestimmten Zeitpunkt nicht wiederhergestellt werden.

Durch ein Differenz-Backup verringert sich die Zeit, die bei der Wiederherstellung einer Datenbank für das Rollforward des Transaktionsprotokoll-Backups benötigt wird.

Backups von SQL Server-Transaktionsprotokollen

Das Transaktionsprotokoll ist eine fortlaufende Aufzeichnung der Transaktionen, die seit dem letzten Backup des Transaktionsprotokolls in der Datenbank ausgeführt wurden. Mithilfe von Transaktionsprotokoll-Backups können Sie die Datenbank auf einen bestimmten zurückliegenden Zeitpunkt bzw. auf den Zeitpunkt des Ausfalls zurücksetzen.

Bei der Wiederherstellung eines Transaktionsprotokoll-Backups führt SQL Server ein Rollforward aller im Transaktionsprotokoll aufgezeichneten Änderungen aus. Wenn SQL Server das Ende des Transaktionsprotokolls erreicht, hat es den genauen Zustand der Datenbank zum Zeitpunkt der Sicherung wiederhergestellt.

Bei der Wiederherstellung der Datenbank setzt SQL Server alle Transaktionen zurück, die zum Zeitpunkt, als der Backup-Vorgang gestartet wurde, nicht abgeschlossen waren.

Für Transaktionsprotokoll-Backups werden in der Regel weniger Ressourcen als für Datenbank-Backups benötigt. Daher können sie häufiger als Datenbank-Backups erstellt werden. Die häufige Erstellung von Backups vermindert das Risiko von Datenverlusten. In OLTP-Umgebungen ("Online Transaction Processing") mit vielen Transaktionen sollten Transaktionsprotokoll-Backups häufiger ausgeführt werden. Transaktionsprotokoll-Backups können nur mit den Wiederherstellungsmodellen "Vollständig" und "Bulk-Protokollierung" verwendet werden.

Das Transaktionsprotokoll kann nicht während eines vollständigen Datenbank-Backups oder Differenz-Backups gesichert werden. Während der Erstellung eines Datei-Backups kann das Transaktionsprotokoll jedoch gesichert werden.

Erstellen Sie niemals ein Transaktionsprotokoll-Backup vor einem Datenbank-Backup, da das Transaktionsprotokoll die Änderungen an der Datenbank enthält, die seit dem letzten Backup vorgenommen wurden.

Löschen Sie niemals manuell Daten aus dem Transaktionsprotokoll, da Sie sonst die Backup-Kette unterbrechen. Wenn ein Transaktionsprotokoll gekürzt wurde, müssen Sie ein vollständiges Datenbank-Backup erstellen, um eine neue Backup-Kette zu erstellen.

Backups von SQL Server-Dateien

Bei einem Datei- oder Dateigruppen-Backup werden einzelne Dateien (oder die Dateien einer Dateigruppe) gesichert. Ein dateibasiertes Modell verkürzt die Wiederherstellungszeit, da Sie nur die beschädigten Dateien - nicht die gesamte Datenbank - wiederherstellen müssen, . Nehmen Sie beispielsweise an, dass eine Datenbank aus mehreren Dateien besteht, die physisch auf unterschiedlichen Laufwerken gespeichert sind, wovon ein Laufwerk

einen Fehler hat. Nur die Datei auf dem beschädigten Laufwerk muss wiederhergestellt und mithilfe des Transaktionsprotokoll-Backups auf den entsprechenden Zustand zurückgesetzt werden.

Datei-Backups und -wiederherstellungsvorgänge müssen gemeinsam mit Transaktionsprotokoll-Backups verwendet werden. Daher können Datei-Backups nur mit den Wiederherstellungsmodellen "Vollständig" und "Bulk-Protokollierung" verwendet werden.

Empfehlungen zum Backup von SQL Server-Datenbanken

Borland empfiehlt Folgendes:

- Verwenden Sie das Modell für die vollständige Wiederherstellung
- Erstellen Sie täglich ein vollständiges Datenbank-Backup. Bei Datenbanken, die insgesamt eine Größe von 3 GB überschreiten, können Sie vollständige Backups auch jeden zweiten Tag erstellen. Wenn Sie vollständige Backups alle zwei Tage erstellen, rät Ihnen Borland dazu, täglich Differenz-Backups zu erstellen.
- Erstellen Sie täglich Transaktionsprotokoll-Backups nach der Fertigstellung des vollständigen oder Differenz-Backups. Zusätzlich hierzu sollten Sie alle vier Stunden ein Transaktionsprotokoll-Backup planen. Kürzen Sie Transaktionsprotokolle niemals manuell.
- Im Falle eines größeren Zusammenbruchs erstellen Sie ein Backup des aktuell aktiven Transaktionsprotokolls. Wenn kein Backup des aktiven Transaktionsprotokolls verfügbar ist (z. B. aufgrund eines Fehlers des Laufwerks, auf dem die Transaktionsprotokolle sich befinden, wenn dieses nicht gespiegelt wird), kann die Datenbank nur mit dem letzten verfügbaren Transaktionsprotokoll-Backup wiederhergestellt werden. Somit kann keine Wiederherstellung eines bestimmten Zeitpunkts erfolgen, der nach dem Zeitpunkt des letzten verfügbaren Transaktionsprotokoll-Backups liegt.

Verwandte Konzepte

Zu sichernde Komponenten
Native-II-Datenspeicher und Hives
StarTeam Backups
Übersicht über die Datenspeicherung
Backups von Oracle-Datenbanken
Backups

Verwandte Verfahrensweisen

Neue Hives erstellen
Optionen für die Datenspeicherung konfigurieren

Backups von Oracle-Datenbanken

Ein Online- oder "Hot"-Backup wird ausgeführt, wenn die Datenbank online und für Lese-/Schreib-Operationen bereit ist. Mit Ausnahme von Oracle-Exporten können Sie Online-Backups nur dann ausführen, wenn sich die Datenbank im ARCHIVELOG-Modus befindet. Ein Offline- oder "Cold"-Backup wird ausgeführt, wenn die Datenbank offline und für die Benutzer nicht verfügbar ist.

Des Weiteren wird in diesem Thema beschrieben, welche Backup-Typen von Oracle unterstützt werden, und es enthält Empfehlungen zum Ausführen von Oracle-Backups.

Oracle-Backup-Typen

Oracle-Datenbankadministratoren verwenden üblicherweise eine oder mehrere der folgenden Optionen zur Sicherung von Oracle-Datenbanken.

Export/Import	Exporte sind "logische" Datenbank-Backups, die logische Definitionen und Daten aus der Datenbank in eine Datei extrahieren. Export-Backups sind plattformübergreifend einsetzbar und können einfach von einem Betriebssystem auf ein anderes verschoben werden.
Cold- oder Offline-Backups	Für diese Backups muss die Datenbankinstanz heruntergefahren werden, damit alle Daten, Protokolle und Steuerungsdateien kopiert werden können.
Hot- oder Online-Backups	Diese Backups werden erstellt, während die Datenbank verfügbar ist und sich im ARCHIVELOG-Modus befindet. Um solche Backups auszuführen, müssen sich die Tablespaces im Backup-Modus befinden und alle mit einem Tablespace verknüpften Dateien müssen gesichert werden. Unbedingt gesichert werden müssen auch die Steuerungsdateien und die archivierten Redo-Log-Dateien.
RMAN-Backups	Sowohl im Offline- als auch im Online-Modus können Datenbankadministratoren die Datenbank mithilfe des RMAN-Dienstprogramms sichern.
Export/Import Data Pump	"Export Pump" und "Import Pump" sind neue Funktionen in Oracle 10g. Expdp und Impdp sind plattformübergreifend einsetzbar und können einfach von einem Betriebssystem auf ein anderes verschoben werden.

Logische Backups von Oracle-Datenbanken

Oracle-Exporte sind "logische" (nicht physische) Datenbank-Backups, die Daten und logische Definitionen aus der Datenbank in eine Datei extrahieren. Bei anderen Backup-Methoden werden in der Regel physische Dateien gesichert. Einer der Vorteile der Exporte ist, dass Sie Tabellen für den Neu-Import einzeln auswählen können. Sie können mit einer wiederhergestellten Export-Datei jedoch keinen Rollforward ausführen. Um eine Datenbank aus einer Export-Datei vollständig wiederherzustellen, müssen Sie fast die gesamte Datenbank neu aufbauen. Bei logischen Backups wird ein Abbild des Datenbank-Schemas zu einem bestimmten Zeitpunkt erstellt.

Offline-/'Cold'-Backups von Oracle-Datenbanken

Als Offline- oder "Cold"-Backup bezeichnet man Backups, die ausgeführt werden, wenn die Datenbank heruntergefahren ist. Sie müssen die Datendateien, die Steuerungsdatei und die Online-Redo-Log-Dateien mithilfe eines entsprechenden Kopierprogramms des Betriebssystems kopieren. Diese Vorgehensweise wird als vollständiges Backup der Datenbank angesehen. Wenn die Datenbank im NOARCHIVELOG-Modus ausgeführt wird, können die nach diesem Backup vorgenommenen Änderungen nicht wiederhergestellt werden. Unabhängig davon, ab die Datenbank im ARCHIVELOG- oder im NOARCHIVELOG-Modus ausgeführt wird, werden alle Transaktionen in Online-Redo-Log-Dateien aufgezeichnet. Wenn die Redo-Logs archiviert werden (ARCHIVELOG-Modus),

ermöglicht es ORACLE, diese Transaktionen nach der Wiederherstellung der beschädigten Dateien anzuwenden (unter der Voraussetzung, dass sich unter den beschädigten Dateien keine aktive Redo-Log-Datei befunden hat).

Wenn das Schema der Datenbank geändert wird, z. B. durch Hinzufügen einer neuen Datendatei, Umbenennen einer Datei bzw. Erstellen oder Entfernen eines erstellten Tablespace, müssen Sie die Datenbank herunterfahren und mindestens die Steuerungsdatei und die neu hinzugefügte Datendatei kopieren. Vorzugsweise sollten Sie ein vollständiges Backup der Datenbank ausführen.

Vor dem Ausführen eines Offline-Backups müssen Sie unbedingt eine Liste aller Oracle-Dateien erstellen, die gesichert werden müssen. Durch Ausführen der folgenden Abfragen erhalten Sie eine vollständige Liste dieser Dateien.

```
select name from sys.v_$datafile;

select member from sys.v_$logfile;

select name from sys.v_$controlfile;
```

Fahren Sie die Datenbank über SQL*Plus oder den Server-Manager herunter. Sichern Sie alle Dateien auf sekundären Speichermedien (z. B. auf Band). Stellen Sie sicher, dass Sie alle Datendateien, Steuerungsdateien und Protokolldateien sichern. Fahren Sie die Datenbank wieder hoch, wenn Sie mit der Sicherung fertig sind.

Hinweis: Wenn die Datenbank im `ARCHIVELOG`-Modus ausgeführt wird, können Sie mithilfe der archivierten Protokolldateien weiterhin ein Rollforward von einem Offline-Backup ausführen. Wenn Sie die Datenbank nicht zu einem geeigneten Zeitpunkt für ein Offline-Backup herunterfahren können, wechseln Sie in den `ARCHIVELOG`-Modus und führen Sie ein Online-Backup aus.

Online-/'Hot'-Backups von Oracle-Datenbanken

Als Online- oder "Hot"-Backups bezeichnet man Sicherungen, die erstellt werden, während die Datenbankinstanz ausgeführt wird. Online-Backups sind an solchen Standorten sehr wichtig, an denen die Datenbankinstanz rund um die Uhr ausgeführt werden muss und die Erstellung von Offline-Backups somit unmöglich ist. Während der Erstellung eines Online-Backups bleibt die Datenbank für Lese- und Aktualisierungsvorgänge verfügbar. Bei dieser Art von Backup muss die Datenbank im ARCHIVELOG-Modus ausgeführt werden. Nur die Datendateien und die aktuelle Steuerungsdatei müssen gesichert werden. Anders als bei Offline-Backups können bei Online-Backups einzelne Tablespaces in beliebigen Kombinationen bei Bedarf gesichert werden. Unterschiedliche Datendateien können zu verschiedenen Zeitpunkten gesichert werden.

Um ein Online-Backup auszuführen, müssen Sie den Tablespace in den Backup-Modus versetzen, bevor Sie die Dateien wie nachfolgend beschrieben kopieren.

```
ALTER TABLESPACE xyz BEGIN BACKUP;

! cp xyfFile1 /backupDir/

ALTER TABLESPACE xyz END BACKUP;
```

Es ist besser, einzelne Tablespaces zu sichern als alle Tablespaces gleichzeitig im Backup-Modus zu laden. Wenn Sie sie einzeln sichern, wird weniger Overhead erzeugt. Nach der Fertigstellung der Tablespace-Backups müssen Sie die Steuerungsdatei wie nachfolgend beschrieben sichern.

```
ALTER SYSTEM SWITCH LOGFILE; -- Protokolldateien wechseln, um Steuerungsdatei-Header zu aktualisieren

ALTER DATABASE BACKUP CONTROLFILE TO '/<Verzeichnis>/control.dbf';
```

Die Häufigkeit von Online-Backups ist umgekehrt proportional zu der Zeit, die für eine Wiederherstellung aufgrund eines beschädigten Mediums benötigt wird. Je älter das Backup, umso mehr Redo-Log-Dateien müssen aufgespielt werden, wodurch die Wiederherstellungszeit verlängert wird. Backup-Strategien sollten vor Verwendung getestet werden, um sicherzustellen, dass die Produktionsdatenbank konsistent wiederhergestellt werden kann.

Borland empfiehlt, Online-Backups zu solchen Zeiten auszuführen, in denen die wenigsten Zugriffe auf die Datenbank erfolgen. Im Backup-Modus schreibt Oracle vollständige Datenbankblöcke anstelle der üblichen Deltas

in die Redo-Log-Dateien. Dies führt zu einer stark erhöhten Datenbankarchivierungs-Aktivität und manchmal sogar zu einem Absturz der Datenbank.

Backups von Oracle-RMAN-Datenbanken

Recovery Manager (RMAN) ist ein Oracle-Tool, mit dem Datenbankadministratoren Oracle-Datenbanken sichern und wiederherstellen können. Mit RMAN können Sie vollständige Backups (im Online- und im Offline-Modus), inkrementelle Backups auf Blockebene sowie Backups der Online-Redo-Logs und Steuerungsdateien ausführen.

Zum Ausführen von RMAN auf einer Datenbank benötigen Sie die Berechtigung SYSDBA. Des Weiteren bieten RMAN-Backups folgende Vorteile:

- Übersichtliche Darstellung aller Backup- und Wiederherstellungsvorgänge
- Verwaltung von zentralen Backup- und Wiederherstellungsprozeduren für das gesamte Unternehmen
- Erkennen von beschädigten Blöcken
- Beschränken der Backups auf die Blöcke, die tatsächlich Daten enthalten. Diese Vorgehensweise kann zu einer signifikanten Verringerung des für Backups benötigen Speicherplatzes führen.
- Unterstützung von inkrementellen Backups. Bei inkrementellen Backups werden nur die Blöcke gesichert, die seit einem zurückliegenden Backup geändert wurden. Dadurch verringert sich der Speicherplatzbedarf und das Backup wird deutlich schneller erstellt. In Oracle 10g gibt es eine neue Funktion namens "block change training". Diese Funktion bietet deutliche Verbesserungen für inkrementelle Backups. Weitere Informationen zur Implementierung dieser Funktion erhalten Sie von Ihrem Datenbankadministrator.

Die folgenden Beispiele zur Backup-Erstellung und Wiederherstellung mit RMAN sind stark vereinfacht und geben Ihnen lediglich einen Einblick in das grundlegende Konzept. Standardmäßig werden Informationen zu Backups bei Oracle in den Steuerungsdateien der Datenbank gespeichert. In der Regel bietet es sich an, eine RMAN-Katalogdatenbank zur Speicherung von RMAN-Metadaten einzurichten. Vor dem Implementieren von RMAN-Backups sollten Sie den *Oracle Backup and Recovery Guide* lesen.

```
rman target sys/*** nocatalog

run {

allocate channel t1 type disk;

backup format '/app/oracle/db_backup/%d_t%t_s%s_p%p' (database);

release channel t1;

}

Beispiel für eine Wiederherstellung mit RMAN:

rman target sys/*** nocatalog

run {

allocate channel t1 type disk;

restore tablespace users;

recover tablespace users;

release channel t1;

}
```

Oracle Export/Import Data Pump

Seit der Version 10g verfügt Oracle über eine Export/Import Data Pump. Die Import-Pump arbeitet zwanzig mal schneller als ein konventionelles Import-Dienstprogramm. Die Dienstprogramme Export und Import Data Pump

erstellen "logische" (anstelle von physischen) Datenbank-Backups, wobei sie Daten und logische Definitionen aus der Datenbank in eine Datei extrahieren. Die Dienstprogramme Export und Import Data Pump können in einem 24/7-Modell nicht eingesetzt werden, da sie keine Rollforward-Funktionen bieten. Export Data Pump erstellt ein Abbild des Datenbank-Schemas zu einem bestimmten Zeitpunkt.

Empfehlungen für Oracle-Datenbank-Backups

Borland empfiehlt, RMAN-Backups zu verwenden, wenn Ihr Unternehmen eine StarTeam-Instanz in einer 24/7-Umgebung betreiben möchte. RMAN wurde über die letzten Jahre hinweg weiterentwickelt und die Oracle Corporation entwickelt weiterhin neue Funktionen, um die Wiederherstellung im Notfall einfacher, zuverlässiger und schneller zu machen.

Verwandte Konzepte

Zu sichernde Komponenten
Native-II-Datenspeicher und Hives
StarTeam Backups
Übersicht über die Datenspeicherung
Backups von SQL Server-Datenbanken
Backups

Verwandte Verfahrensweisen

Neue Hives erstellen
Optionen für die Datenspeicherung konfigurieren

Anpassung

Die Themen in diesem Abschnitt beschreiben, wie Sie StarTeam an die Anforderungen Ihres Unternehmens anpassen.

E-Mail-Unterstützung und angepasste E-Mail-Benachrichtigungen

Um die Vorteile von E-Mail-Benachrichtigungen nutzen zu können, müssen Sie die E-Mail-Unterstützung und die E-Mail-Benachrichtigung im Register **Allgemein** des Dialogfelds **Server konfigurieren** im Fenster "Serveradministration" aktivieren. Dieses Thema beschreibt die konzeptionellen Informationen zur E-Mail-Unterstützung, zu E-Mail-Benachrichtigungen und angepassten E-Mail-Benachrichtigungen für StarTeam-Server.

Vom Client berechnete Felder können in benutzerdefinierten E-Mail-Benachrichtigungen oder mit Notification Agent nicht verwendet werden.

E-Mail-Unterstützung

Wenn die E-Mail-Unterstützung für eine Serverkonfiguration aktiviert ist, können Benutzer in StarTeam Elementeigenschaften per E-Mail an andere Benutzer versenden. Um die E-Mails empfangen zu können, müssen die Empfänger das Programm nicht ausführen.

Benutzer erhalten automatisch E-Mail-Benachrichtigungen, wenn ihre exklusiven Sperren für Elemente umgangen werden. Benutzer können Sperren nur umgehen, wenn sie über die erforderlichen Zugriffsrechte und Berechtigungen hierfür verfügen.

Sie können das Programm auch so konfigurieren, dass bei bestimmten Ereignissen automatische E-Mail-Benachrichtigungen versendet werden. Abhängig von der Serverkonfiguration und der Systemrichtlinie können Sie Folgendes auswählen:

- Mitglieder der Gruppe "System Managers" erhalten eine E-Mail, wenn ein Fehler zum Serverprotokoll hinzugefügt wird.
- Mitglieder der Gruppe "Security Administrators" erhalten eine E-Mail, wenn ein Anmeldefehler auftritt.
- Alle Benutzer erhalten automatische Benachrichtigungen über Elemente, für die sie zuständig oder deren Empfänger sie sind.

Hinweis: Wenn der Empfänger eines Elements oder einer Benachrichtigung eine falsch formatierte E-Mail-Adresse hat, wird ein Eintrag ins Serverprotokoll geschrieben, der angibt, dass beim Senden der E-Mail an die Adresse ein Problem aufgetreten ist. Wenn eine E-Mail-Adresse richtig formatiert, aber ungültig ist (z. B. "junk@place.com"), wird die E-Mail an alle anderen gültigen Empfänger gesendet und der Sender erhält vom E-Mail-System die Meldung, dass die E-Mail nicht an den ungültigen Empfänger gesendet werden konnte.

E-Mail-Benachrichtigung

Wenn Sie die E-Mail-Benachrichtigung aktivieren, erhalten Benutzer in folgenden Fällen automatisch E-Mails:

- Der Wert des Felds *Zuständigkeit* ändert sich in einer Änderungsanforderung
- Wenn ein Feld für eine Anforderung oder Aufgabe geändert wurde, für die der Benutzer verantwortlich ist.
- Wenn sich ein beliebiges Feld eines Themas ändert, für das der Benutzer als Empfänger eingetragen ist. (Wenn ein Thema über keinen Empfänger verfügt, erhält niemand eine Benachrichtigung.)

Die Teammitglieder müssen keinen Client ausführen, um Benachrichtigungen zu empfangen, da die E-Mail-Benachrichtigung Client-unabhängig ist.

Standardnachrichten, die an Empfänger automatischer E-Mail-Benachrichtigungen gesendet werden, werden basierend auf der Ländereinstellung des Servers lokalisiert. Wenn die Länderkennung eines Servers beispielsweise fr-FR lautet, wird die Nachricht in Französisch gesendet, da für den Server eine französische Version vorhanden ist. Wenn es für eine Ländereinstellung keine Übersetzung gibt, wird die Nachricht in Englisch gesendet.

Tipp: Die mit der jeweiligen Serverkonfiguration verwendete Sprache kann geändert werden, indem `NotificationLocale` zu dem für die Konfiguration reservierten Abschnitt der Datei `starteam-server-configs.xml` hinzugefügt wird. Wenn Sie beispielsweise `NotificationLocale=ja` hinzufügen, werden die Nachrichten in Japanisch gesendet.

Benutzer könnten E-Mail-Nachrichten von anderen Benutzern (die mit dem Befehl **Senden an** gesendet werden) mit E-Mail-Benachrichtigungen verwechseln, da die Vorlagen für E-Mail-Nachrichten sehr ähnlich sind. Daher bietet es sich an, die Benutzer wissen zu lassen, wenn Sie die automatische E-Mail-Benachrichtigung aktivieren, und diesen die Unterschiede zwischen den zwei E-Mail-Formaten und den zwei Benachrichtigungstypen zu erklären.

Hinweis: Sie können die E-Mail-Benachrichtigungen dynamisch pro Serverkonfiguration, pro Projekt oder pro Komponente anpassen. Bearbeiten Sie die Vorlagen, die sich in Ihrem Repository im Ordner *Notifications* befinden. Sie können die in der StarTeam-Datenbank gespeicherten Felder mit den benutzerdefinierten Vorlagen verwenden. Eine Liste der Felder finden Sie unter dem Link "Referenz" am Ende dieses Themas.

Benutzerdefinierte E-Mail-Benachrichtigungen

Sie können den StarTeam-Server so konfigurieren, dass *angepasste* automatische E-Mail-Benachrichtigungen pro Serverkonfiguration, pro Projekt oder pro Komponente versendet werden. Sie können Ihre eigenen text- oder HTML-basierten Nachrichtenvorlagen entwerfen oder die neuen Standardvorlagen von Borland verwenden, die sich im Ordner *Notifications*, einem Unterordner der Serverinstallation, befinden. Alle E-Mail-Benachrichtigungen (sowohl einfacher Text als auch HTML) werden in der UTF-8-Codierung versendet.

Sie können für die folgenden Komponenten angepasste E-Mail-Vorlagen für die Verwendung mit E-Mail-Benachrichtigungen verwenden:

- Änderungsanforderung
- Task
- Thema
- Anforderung

Um die Vorteile von E-Mail-Benachrichtigungen nutzen zu können, müssen Sie die E-Mail-Unterstützung und die E-Mail-Benachrichtigung im Register **Allgemein** des Dialogfelds **Server konfigurieren** im Fenster "Serveradministration" aktivieren. Wenn Sie die Vorlagen oder Konfigurationsdateien für E-Mail-Benachrichtigungen nicht anpassen möchten und die E-Mail-Benachrichtigung auf dem Server aktiviert ist, sehen Benutzer die standardmäßigen E-Mail-Benachrichtigungen, die StarTeam in früheren Versionen verwendet hat.

Wenn eine Serverkonfiguration das erste Mal gestartet wird, wird der Inhalt des Ordners "Notifications" im Installationsverzeichnis in das Repository für die Serverkonfiguration in den entsprechenden *Notifications*-Ordner kopiert. Sie können Anpassungen an den Standardvorlagen im *Notifications*-Ordner vornehmen, der sich im Repository der Serverkonfiguration befindet. Die vordefinierten E-Mail-Benachrichtigungsdateien bestehen aus mehreren XML-Konfigurationsdateien auf Komponentenebene – eine für jede gewünschte Komponente und eine beliebige Anzahl von Vorlagen für E-Mail-Nachrichtentext, die beliebig benannt werden können. Die Konfigurationsdateien *müssen* jedoch wie folgt benannt werden:

- `ChangeRequest.xml`
- `Requirement.xml`
- `Task.xml`
- `Topic.xml`

Die vordefinierten Vorlagen für den E-Mail-Nachrichtentext heißen wie folgt:

- `itemTypeAbbr-new.txt`
- `itemTypeAbbr-modified.txt`
- `itemTypeAbbr-new.html`
- `itemTypeAbbr-modified.html`

Wobei `itemTypeAbbr` `cr`, `req`, `task` oder `topic` entspricht.

Bei jedem Start der Serverkonfiguration wird der Inhalt des Ordners *Notifications* überprüft. Wenn die Konfigurationsdateien (.xml) ungültig sind und die E-Mail-Benachrichtigung für die Serverkonfiguration aktiviert ist, gibt der Server eine Fehlermeldung im Serverprotokoll aus und die Serverkonfiguration kann nicht gestartet werden.

Sie können auch dynamische Aktualisierungen an den Nachrichtenvorlagen im Repository-Ordner *Notifications* vornehmen, ohne die Serverkonfiguration neu zu starten. Der Server überprüft die Konfiguration und die Nachrichtenvorlagendateien alle zwei Minuten auf Änderungen und wendet gültige Änderungen, die er in den Dateien findet, sofort an.

Wenn der Server eine beschädigte Konfigurations- und/oder Vorlagendatei findet, während die Serverkonfiguration ausgeführt wird, wird eine vordefinierte E-Mail-Nachricht an die Admin-Gruppe gesendet. Die E-Mail-Benachrichtigung ist erst dann wieder verfügbar, wenn Sie eine gültige Konfiguration im Ordner *Notifications* wiederherstellen. Wenn eine der Dateien im Ordner *Notifications* einen ungültigen Status aufweist, sendet der Server den Benutzern die standardmäßigen E-Mail-Benachrichtigungen, die StarTeam in den früheren Versionen verwendet hat.

Hinweis: Weitere Informationen und Beschreibungen der Vorlagendateien für den Nachrichtentext für eine Änderungsanforderung finden Sie unter dem Link im Abschnitt "Referenz" am Ende dieses Themas.

In Vorlagen für E-Mail-Benachrichtigungen verwendete StarTeam-Felder

Jede der Beispielvorlagen im Ordner *Notifications* in Ihrem Repository enthält Felder, die Sie in Ihren eigenen angepassten Vorlagen verwenden können. StarTeam verwendet drei Feldtypen:

- In der Datenbank gespeicherte Felder
- Vom Client berechnete Felder
- Vom Server berechnete Felder

Hinweis: Vom Client oder Server berechnete Felder können in angepassten Vorlagen für E-Mail-Benachrichtigungen nicht verwendet werden. Die Vorlagen erkennen *nur die in der Datenbank gespeicherten Felder*.

In Vorlagen für E-Mail-Benachrichtigungen eingebettete Bilder

Es ist nicht möglich, Bilder in die HTML-Vorlagen für E-Mail-Nachrichten einzubetten. Sie können jedoch eine URL eines Bilds auf einer Website verwenden, auf die Benutzer zugreifen können. Das Bild wird in diesem Fall als *extern* betrachtet. Ob es angezeigt wird, ist von den Anwendungseinstellungen des E-Mail-Clients des Benutzers abhängig.

Verwandte Verfahrensweisen

E-Mail-Unterstützung und -Benachrichtigung konfigurieren
E-Mail-Benachrichtigungen pro Projekt und pro Komponente konfigurieren

Verfahren

Dieser Abschnitt beschreibt alle Aufgaben in Verbindung mit der Verwaltung und dem Einsatz von StarTeam.

In diesem Abschnitt

Server lizenzieren
Dieser Abschnitt beschreibt Aufgaben im Zusammenhang mit der Lizenzierung.

Sicherheitsoptionen festlegen
In diesem Abschnitt sind Verfahrensweisen zum Festlegen von Sicherheitsoptionen beschrieben.

Server migrieren
Dieser Abschnitt beschreibt Verfahrensweisen zum Migrieren von Daten zwischen zwei Servern.

Benutzer und Gruppen verwalten
Dieser Abschnitt beschreibt Vorgehensweisen zum Verwalten von Benutzern und Gruppen.

Passwörter verwalten
Dieser Abschnitt beschreibt Vorgehensweisen zum Verwalten von Passwörtern.

Zugriffsrechte und Gruppenberechtigungen verwalten
Dieser Abschnitt beschreibt Vorgehensweisen zum Verwalten von Zugriffsrechten und Gruppenberechtigungen.

Protokoll- und Initialisierungsdateien verwalten
Dieser Abschnitt beschreibt Vorgehensweisen zum Verwalten von Protokoll- und Initialisierungsdateien.

Informationen sichern
In diesem Abschnitt sind Verfahrensweisen zum Sichern von Informationen beschrieben.

Daten aus Auscheckvorgängen verfolgen
In diesem Abschnitt werden Vorgehensweisen beim Verfolgen von Daten aus Auscheckvorgängen mithilfe des Checkout Trace-Dienstprogramms beschrieben.

Mit Serverkonfigurationen arbeiten
In diesem Abschnitt werden Verfahrensweisen beim Arbeiten mit Serverkonfigurationen beschrieben.

Serverkonfigurationsoptionen ändern
In diesem Abschnitt sind Verfahrensweisen beim Anpassen von Serverkonfigurationsoptionen beschrieben.

Optionen für die Datenspeicherung konfigurieren
In diesem Abschnitt sind Verfahrensweisen beim Konfigurieren von Datenspeicherungsoptionen beschrieben.

Server lizenzieren

Diese Themen beschreiben die Vorgehensweisen zum Einrichten und Verwalten von StarTeam Server - Windows-Lizenzen.

In diesem Abschnitt

Benutzern Lizenzen zuweisen

Um mit StarTeam arbeiten zu können, benötigen Benutzer eine personengebundene Lizenz oder eine Lizenz für gleichzeitige Benutzer. Die Vorgabe für Benutzer ist die Verwendung von Lizenzen für gleichzeitige Benutzer. Der StarTeam-Server-Administrator weist vorhandenen oder neuen Benutzern mithilfe des **Benutzer-Managers** im Serveradministrations-Tool Lizenzen zu.

Im **Benutzer-Manager** können Sie das Dialogfeld **Benutzereigenschaften** oder das Kontextmenü zum Zuweisen von Lizenzen verwenden. In der Regel sollten Sie das Kontextmenü für in größerer Menge auszuführende Aktionen verwenden und das Dialogfeld **Benutzereigenschaften**, um Lizenzen einzeln an Benutzer zu vergeben. Lizenzen können auch mithilfe von Borland LDAP QuickStart Manager zugewiesen werden (normalerweise in größerer Menge, aber auch einzeln möglich). Für welche Möglichkeit Sie sich entscheiden, hängt von der Aktion ab, die Sie durchführen möchten, wie nachfolgend dargestellt:

- Wenn Sie einen neuen Benutzer hinzufügen und die Daten zu dem Benutzer eingeben, können Sie dabei auch eine Lizenz zuweisen. Dies erfolgt normalerweise im Dialogfeld **Eigenschaften für den neuen Benutzer**.
- Wenn Sie ein Upgrade durchführen und einer neuen .slip-Lizenzdatei eine Gruppe vorhandener Benutzer für das neue Release zuweisen müssen, können Sie die entsprechenden Benutzer gleichzeitig auswählen und einer .slip-Datei zuweisen. In diesem Fall würde man das Kontextmenü verwenden.
- Wenn Sie StarTeam evaluiert haben und dann native Lizenzen oder Lizenzen zur Verwendung mit einem Lizenzserver erworben haben, können Sie alle aus dem Evaluierungszeitraum vorhandenen Benutzer aus Ihrer Produktionsserverkonfiguration auswählen und sie einem Lizenztyp oder einer .slip-Lizenzdatei zuweisen. In diesem Fall würde man das Kontextmenü verwenden.
- Wenn eine Gruppe von Benutzern StarTeam nicht mehr verwenden soll, können Sie diese gleichzeitig auswählen und ihren Lizenztyp in **Nicht zugewiesen** ändern.

Hinweis: Die personenbezogenen Lizenzen und die Lizenzen für gleichzeitige Benutzer unterscheiden sich nicht von den Lizenzen in früheren Versionen von StarTeam.

So weisen Sie vorhandenen Benutzern Lizenzen zu

1. Öffnen Sie das Serveradministrations-Tool, indem Sie **Start** ▸ **Programme** ▸ **StarTeam** ▸ **StarTeam Server 2009** ▸ **StarTeam-Server** wählen.
2. Wählen Sie in der Serverliste eine Serverkonfiguration aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun. Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.
3. Führen Sie einen der folgenden Schritte aus:
    - Klicken Sie im unteren linken Fenster auf **Konten**. Klicken Sie anschließend auf die Verknüpfung **Benutzer-Manager**.
    - Wählen Sie **Tools** ▸ **Konten** ▸ **Benutzer-Manager**.

    Der **Benutzer-Manager** wird angezeigt.
4. Wählen Sie die gewünschten Benutzer aus.
5. Klicken Sie mit der rechten Maustaste, um das Kontextmenü zu öffnen, und wählen Sie **Eigenschaften**, um das Dialogfeld **Benutzereigenschaften** anzuzeigen.
6. Wählen Sie den Lizenztyp aus dem Dropdown-Listenfeld "Lizenz":
    - (optional) Die Lizenznummer einer oder mehrerer Borland-Lizenzserver-.slip-Dateien für eine personenbezogene Lizenz oder eine Lizenz für gleichzeitige Benutzer.
    - **StarTeam - Personengebundene Lizenz**. Dem Benutzer wird eine bestimmte Lizenz zugewiesen.

- **StarTeam - Lizenz für gleichzeitige Benutzer**. Dem Benutzer wird bei der Anmeldung bei StarTeam eine der "frei verfügbaren" Lizenzen zugewiesen.
- **Nicht zugewiesen**. Wählen Sie diesen Lizenztyp, wenn ein Benutzer keine Lizenz besitzt.

7 Möglicherweise müssen Sie die Eigenschaften für den Benutzer bearbeiten, um den Benutzernamen in den Netzwerk-Anmeldenamen zu ändern.

Hinweis: Die Statuszeile unten im Fenster "Benutzer-Manager" zeigt Lizenzstatistiken an, darunter die Anzahl derzeit verfügbarer personengebundener Lizenzen.

So weisen Sie einem neuen Benutzer eine Lizenz zu

1 Wählen Sie im **Benutzer-Manager** den Schalter **Neuer Benutzer**.

Das Dialogfeld **Eigenschaften für den neuen Benutzer** wird angezeigt.

2 Wählen Sie im Register **Allgemein** im Dropdown-Listenfeld **Lizenz** einen Lizenztyp aus.

- **StarTeam - Personengebundene Lizenz**. Dem Benutzer wird eine bestimmte Lizenz zugewiesen.
- **StarTeam - Lizenz für gleichzeitige Benutzer**. Dem Benutzer wird bei der Anmeldung bei StarTeam eine der "frei verfügbaren" Lizenzen zugewiesen.
- **Nicht zugewiesen**. Wählen Sie diesen Lizenztyp, wenn ein Benutzer keine Lizenz besitzt.

Die Vorgabe ist "StarTeam - Lizenz für gleichzeitige Benutzer".

3 Geben Sie die restlichen Daten in das Register **Allgemein** und die anderen Register ein. Vergessen Sie nicht, im Textfeld **Benutzername** des Registers **Anmeldung** den Netzwerk-Anmeldenamen anzugeben.

4 Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften für den neuen Benutzer** zu schließen.

Verwandte Konzepte

Lizenz - Übersicht

Verwandte Verfahrensweisen

Personengebundene Lizenzen verwalten
Lizenzserver einrichten
Benutzer und Gruppen verwalten

Evaluierungslizenzen verwenden

Wenn Sie den StarTeam Server - Windows zum ersten Mal ausführen, wird eine Evaluierungslizenz für StarTeam Enterprise Advantage erstellt, die StarTeam-Edition mit den meisten Funktionen.

Stellen Sie vor Ablauf des 30-tägigen Produkt-Evaluierungszeitraums sicher, dass Sie das Produkt registrieren oder den Evaluierungszeitraum verlängern. Anderenfalls sind, wenn Clients auf eine von einem StarTeam-Server verwaltete Serverkonfiguration zugreifen und der Zeitraum abgelaufen ist, keine Komponenten (wie z. B. die Komponenten **Datei** oder **Änderungsanforderung**) verfügbar, und im StarTeam Cross-Platform Client sind im oberen und unteren Fenster keine Register vorhanden.

So verlängern Sie den Evaluierungszeitraum für StarTeam Server - Windows

1. Beziehen Sie einen Schlüssel zur Verlängerung der Evaluierung, indem Sie sich über die Webseite http://www.borland.com/us/company/how-to-buy.html mit Borland in Verbindung setzen.
2. Öffnen Sie das Serveradministrations-Tool, indem Sie **Start** ▸ **Programme** ▸ **StarTeam** ▸ **StarTeam Server 2009** ▸ **StarTeam-Server** wählen.
3. Wählen Sie in der Menüleiste **Hilfe** ▸ **Info**. Das Dialogfeld **Info über StarTeam-Server** wird angezeigt.
4. Wählen Sie im linken Fenster des Dialogfelds das Element **Lizenz**.
5. Klicken Sie auf **Testphase verlängern**. Das Dialogfeld **Testphase verlängern** wird angezeigt.
6. Geben Sie den Schlüssel für die Testphase ein und klicken Sie auf **OK**.
7. Schließen Sie das Dialogfeld **Info über StarTeam-Server**.

Verwandte Konzepte

Lizenz - Übersicht

Verwandte Verfahrensweisen

Lizenzserver einrichten

Lizenzdateien (.slip) speichern

Nachdem Sie von Borland eine Lizenzzertifikats-E-Mail mit Lizenzierungsinformationen erhalten haben (dies wird von einem Vertriebsmitarbeiter veranlasst), müssen Sie den Lizenzserver installieren und die von Borland erhaltenen Lizenzen hosten. Dazu müssen Sie auf eine Borland-Website gehen und Borland-Lizenzdateien, genannt .slip-Dateien, wie hier beschrieben herunterladen.

So speichern Sie die .slip-Lizenzdateien

1. Rufen Sie den Link aus der Lizenzzertifikats-E-Mail auf und laden Sie von der Borland-Website alle .zip-Dateien herunter, die die .slip-Dateien enthalten. Gehen Sie dazu nach den Anweisungen im Internet vor.
2. Kopieren Sie die einzelnen `concurrent_.slip`- und/oder `named_.slp` -Dateien in das Verzeichnis `C:\Programme\Borland\StarTeam Server 2009\License`.
3. Kopieren Sie alle `server_.slip`-Dateien nach `C:\Borland\BLS4\conf`.

Hinweis: Der Name des Ordners "BLS4" ändert sich gegebenenfalls mit der jeweiligen Version von Borland License Server, die Sie verwenden. Außerdem müssen möglicherweise, wenn Sie FLEXlm anstelle von Borland License Server verwenden, die server_.slip-Dateien an einem anderen Ort installiert werden. Lesen Sie dies in der FLEXlm-Server-Dokumentation nach.

Beim Programmstart sucht StarTeam-Server nach .slip-Dateien und legt die gefundenen Daten im Speicher ab. Neue .slip-Dateien werden erst beim nächsten Programmstart erkannt.

Sobald Sie die .slip-Dateien in den Ordner `\License` kopiert haben und der StarTeam-Server neu gestartet wurde, kann der **Benutzer-Manager** im Serveradministrations-Tool Informationen zu den .slip-Dateien anzeigen und ein Administrator kann Benutzern Lizenzen aus diesen .slip-Dateien zuweisen.

Verwandte Konzepte

Lizenz - Übersicht

Verwandte Verfahrensweisen

Benutzern Lizenzen zuweisen
Personengebundene Lizenzen verwalten
Lizenzserver einrichten

Lizenzserver einrichten

Sie können zwischen der Verwendung des Borland License Server (BLS) und der nativen, bereits aus anderen Versionen bekannten StarTeam-Lizenzen wählen. Wenn Sie den Lizenzserver einsetzen, müssen die Benutzer ihre Netzwerk-Anmeldenamen als StarTeam-Benutzernamen verwenden. In diesem Abschnitt sind die Schritte beschrieben, die der Administrator ausführen muss, um einen Lizenzserver einzurichten.

So richten Sie einen Lizenzserver ein

1. Wenn Sie der StarTeam-Administrator sind, erhalten Sie normalerweise per E-Mail Lizenzdaten von Borland (dies wird von einem Vertriebsmitarbeiter veranlasst).
2. Installieren Sie den Lizenzserver (die Vorgehensweise wird in der Lizenzserver-Dokumentation beschrieben).
3. Speichern Sie die Lizenzdateien (dazu müssen Sie auf eine Borland-Website gehen und die Borland-Lizenzdateien mit der Erweiterung ".slip" herunterladen).
4. Legen Sie die .slip-Dateien im Ordner `/License` ab. Dieser ist ein Unterverzeichnis des Installationsordners `StarTeam Server 2009`.
5. Konfigurieren Sie den Lizenzserver für Benutzer (dies wird in der Lizenzserver-Dokumentation beschrieben).
6. Mit dem StarTeam Serveradministrations-Tool können Sie folgende Aktionen ausführen:
   - Benutzernamen in Netzwerk-Anmeldenamen ändern.
   - Durch Festlegen der Lizenzoptionen Benutzer bestimmten Lizenzen zuweisen.

Beim Programmstart sucht StarTeam-Server nach .slip-Dateien und legt die gefundenen Daten im Speicher ab. Neue .slip-Dateien werden erst beim nächsten Programmstart erkannt.

Wenn sich ein Benutzer über einen StarTeam-Client anmeldet, teilt der Server dem Client mit, auf welche Funktionen der Benutzer gemäß seiner Lizenz zugreifen darf. Wenn dem Benutzer eine Lizenz per .slip-Datei zugewiesen wurde, sich diese jedoch nicht mehr im Ordner `/License` befindet, zeigt StarTeam-Server eine Fehlermeldung an. Wenn der Lizenztyp des Benutzers **Nicht zugewiesen** ist, kann sich dieser nicht anmelden und der StarTeam-Server gibt eine Exception zurück.

Hinweis: Wenn Sie einen Lizenzserver verwenden, werden Lizenzen für gleichzeitige Benutzer sofort vom StarTeam-Server ausgegeben, möglicherweise dauert es jedoch einige Minuten, bis der Lizenzserver dies erkennt. StarTeam-Server gibt mit einem Zeitintervall, das in der .slip-Lizenzdatei festgelegt ist, neue Informationen über die Lizenznutzung an den Lizenzserver weiter. Der Lizenzserver erkennt erst bei der nächsten Aktualisierung, die für eine Lizenz stattfindet, dass die Lizenz ausgegeben wurde.

Verwandte Konzepte

Lizenz - Übersicht

Verwandte Verfahrensweisen

Personengebundene Lizenzen verwalten
Lizenzdateien (.slip) speichern
Benutzern Lizenzen zuweisen

Native Lizenzen verwenden

Wenn Sie den StarTeam-Server zum ersten Mal ausführen, wird eine Evaluierungslizenz für StarTeam Enterprise Advantage erstellt, die StarTeam-Edition mit den meisten Funktionen. Stellen Sie vor Ablauf des 30-tägigen Produkt-Evaluierungszeitraums sicher, dass Sie das Produkt registrieren oder den Evaluierungszeitraum verlängern.

Dieses Thema beschreibt, wie Sie StarTeam Server unter Verwendung des Serveradministrations-Tool und der Befehlszeile lizenzieren. Diese Art der Lizenzierung wird als native Lizenzierung bezeichnet.

So registrieren Sie eine native Lizenz mit dem Serveradministrations-Tool

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool.
2. Wählen Sie im Hauptmenü **Hilfe** ▸ **Info**. Das Dialogfeld **Info über StarTeam-Server** wird geöffnet.
3. Wählen Sie im linken Fenster des Dialogfelds den Knoten **Lizenz**.
4. Wenn Sie noch keine Lizenz eingegeben haben, müssen Sie den Evaluierungsschlüssel löschen, indem Sie diesen auf der rechten Seite des Fensters auswählen und auf **Löschen** klicken.
5. Klicken Sie auf **Registrieren**. Das Dialogfeld **Serverregistrierung** wird geöffnet.
6. Geben Sie in die Textfelder "Seriennummer" und "Zugriffsschlüssel" die richtigen Zahlen ein.

   Hinweis: Bei Seriennummern muss die Groß-/Kleinschreibung beachtet werden, bei Zugriffsschlüsseln nicht.

7. Klicken Sie auf **OK**.
8. Schließen Sie das Dialogfeld **Info über StarTeam-Server**.

So registrieren Sie eine native Lizenz an der Befehlszeile

1. Öffnen Sie eine Befehlszeile und navigieren Sie zum Home-Installationsordner für StarTeam-Server. Beispiel: `C:\Programme\Borland\StarTeam-Server xxxx`.
2. Geben Sie in der Befehlszeile Folgendes ein: `starteamserver -Seriennummer -Zugriffsschlüssel`

Hinweis: Sie können StarTeam-Server nicht lizenzieren, wenn eine der Serverkonfigurationen als Windows-Dienst ausgeführt wird.

Wenn Sie die registrierte Lizenz ändern, während ein Benutzer auf seiner Workstation ein StarTeam-Projekt geöffnet hat, wird die Änderung für diesen Benutzer wirksam, nachdem er das Projektfenster geschlossen und erneut geöffnet hat.

Wenn Sie einen StarTeam-Server nach Verwendung einer Evaluierungslizenz für die Enterprise Advantage-Version als "Enterprise" lizenzieren, ändert sich der Funktionsumfang. Wenn Sie beispielsweise in der Evaluierungsphase Anforderungen erstellt haben und den Server anschließend mit einer anderen als der Enterprise Advantage-Version lizenzieren, wird das Register "Anforderungen" nicht mehr angezeigt.

Verwandte Konzepte

Lizenz - Übersicht

Verwandte Verfahrensweisen

Lizenzserver einrichten
Serveradministrations-Tool öffnen

Personengebundene Lizenzen verwalten

Benutzer verfügen entweder über personengebundene Lizenzen oder Lizenzen für gleichzeitige Benutzer. Eine personengebundene Lizenz kann nur von dem Benutzer verwendet werden, dem die Lizenz zugewiesen wurde. Bei Lizenzen für gleichzeitige Benutzer hingegen teilen sich Benutzer die Lizenzen und können sich anmelden, solange Lizenzen für gleichzeitige Benutzer verfügbar sind. Benutzern, die personengebundene Lizenzen erhalten, ist der Zugriff auf den Server garantiert.

Sie können eine beliebige Anzahl von Benutzern hinzufügen, der Zugriff auf den Server wird jedoch nur den Benutzern mit personengebundenen Lizenzen oder Benutzern gewährt, denen bei der Anmeldung Lizenzen für gleichzeitige Benutzer zugewiesen werden. Personengebundene Lizenzen müssen im Serveradministrations-Tool **Benutzer-Manager** bestimmten Benutzern zugewiesen werden. Vor den Namen der Benutzer, die über personengebundene Lizenzen verfügen, wird ein Ankersymbol angezeigt. Vor dem Zuweisen von personengebundenen Lizenzen müssen Sie die betreffenden Benutzer hinzufügen.

Dem Server-Administrator wird automatisch eine personengebundene Lizenz zugewiesen, die nicht entfernt werden kann. Dabei handelt es sich um eine kostenfreie Lizenz, die nicht in der Anzahl verfügbarer personengebundener Benutzerlizenzen enthalten ist. Nachdem der Server eine Lizenz erhalten hat, können personengebundene Lizenzen zugewiesen werden.

Tipp: Die **Benutzer-Manager**-Statusleiste zeigt an, wieviele personengebundene Lizenzen und wieviele Lizenzen für gleichzeitige Benutzer gegenwärtig verwendet werden.

So weisen Sie eine personengebundene Benutzerlizenz zu

1. Öffnen Sie das Serveradministrations-Tool, indem Sie **Start** ▸ **Programme** ▸ **StarTeam** ▸ **StarTeam Server 2009** ▸ **StarTeam-Server** wählen.
2. Wählen Sie in der Serverliste eine Serverkonfiguration aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun. Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.
3. Führen Sie im Serveradministrations-Tool einen der folgenden Schritte aus:
   - Klicken Sie im unteren linken Fenster auf **Konten**. Klicken Sie anschließend auf die Verknüpfung **Benutzer-Manager**.
   - Wählen Sie **Tools** ▸ **Konten** ▸ **Benutzer-Manager**.

   Der **Benutzer-Manager** wird angezeigt.
4. Wählen Sie den Benutzer aus, dem eine personengebundene Lizenz zugewiesen werden soll.

   Hinweis: Wenn der Benutzer nicht angezeigt wird, müssen Sie möglicherweise eine bestimmte Gruppe auswählen oder das Auswahlfeld **Benutzer in allen nachfolgenden Gruppen anzeigen** aktivieren.
5. Klicken Sie mit der rechten Maustaste und wählen Sie im Kontextmenü **Lizenz zuweisen** ▸ **Personengebundene Benutzerlizenz hinzufügen**.

Hinweis: Wenn Sie Lizenzdateien für personenbezogene Lizenzen oder Lizenzen für gleichzeitige Benutzer vom Borland License Server heruntergeladen haben, zeigt das Kontextmenü die Lizenznummern der einzelnen Dateien an.

Nachdem einem Benutzer eine personengebundene Lizenz zugewiesen wurde, wird vor seinem Benutzernamen ein Anker angezeigt.

Hinweis: Wenn Sie den Typ der Lizenz eines Benutzers ändern, wird die Änderung erst wirksam, wenn sich der Benutzer das nächste Mal anmeldet. Sie können die Lizenzänderung sofort wirksam machen, indem Sie die Abmeldung der von der Änderung betroffenen Benutzer erzwingen.

So entfernen Sie eine personengebundene Benutzerlizenz:

1. Wählen Sie im **Benutzer-Manager** mindestens einen Benutzer aus.
2. Klicken Sie mit der rechten Maustaste und wählen Sie im Kontextmenü **Lizenz zuweisen** ▸ **Personengebundene Benutzerlizenz entfernen**.

Hinweis: Wenn Sie eine personengebundene Lizenz entfernen, erhält der Benutzer stattdessen automatisch eine Lizenz für gleichzeitige Benutzer.

Verwandte Konzepte

Lizenz - Übersicht

Verwandte Verfahrensweisen

Benutzern Lizenzen zuweisen
Lizenzserver einrichten
Benutzer und Gruppen verwalten

Sicherheitsoptionen festlegen

In diesem Abschnitt sind Verfahrensweisen zum Festlegen von Sicherheitsoptionen beschrieben.

In diesem Abschnitt

Anzahl der möglichen Anmeldeversuche konfigurieren

Sie können die Sicherheit Ihrer Projekte erhöhen, indem Sie Einstellungen für Anmeldefehler und Zeitlimits für Anmeldevorgänge festlegen. Eine Ursache für Anmeldefehler kann sein, dass Hacker versuchen, Benutzerpasswörter auszuspionieren. In solchen Fällen sollten Sie die IP-Adresse des Systems möglicherweise ändern, um es den Angreifern zu erschweren, die Serverkonfiguration zu finden und ihre Angriffe zu wiederholen. Gegebenenfalls sollten Sie auch die Benutzernamen aller Benutzer des Systems ändern.

Sie können die Serverkonfiguration so konfigurieren, dass Mitglieder der Gruppe "Security Administrators" per E-Mail über fehlgeschlagene Anmeldungen benachrichtigt werden.

Hinweis: Diese Operation kann nur bei aktiviertem Server ausgeführt werden.

So legen Sie ein Limit für Anmeldeversuche fest

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.
2. Wählen Sie in der Serverliste eine Serverkonfiguration aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.
3. Wählen Sie im Hauptmenü **Tools** ▸ **Konten** ▸ **Systemrichtlinie**. Das Dialogfeld **Systemrichtlinie** wird geöffnet.
4. Wählen Sie das Register **Fehler bei der Anmeldung**.
5. Wählen Sie eine der folgenden Optionen für **Fehlschläge bei der Anmeldung** aus:
   - **Ignorieren**: Fehler bei der Anmeldung werden nicht berücksichtigt.
   - **Konto sperren nach ___ Fehlschlägen**: Geben Sie die Anzahl der zulässigen Fehlschläge bei der Anmeldung ein.
6. Wählen Sie eine der folgenden Option unter **Sperrdauer** aus:
   - **Dauerhaft**: Wenn diese Option ausgewählt ist, kann nur der Administrator die Sperre für den Benutzer aufheben.
   - **Sperre beibehalten für ___ Minuten**: Geben Sie an, wie viele Minuten die Sperre andauern soll. Nach der angegebenen Sperrfrist kann sich der Benutzer erneut anmelden.
7. Um Mitglieder der Gruppe "Security Administrators" über StarTeam-Benutzer zu informieren, deren Anmeldung nicht erfolgreich war, aktivieren Sie das Auswahlfeld **Per E-Mail**.
8. Klicken Sie auf **OK**, um die Änderungen zu übernehmen und das Dialogfeld zu schließen.

Verwandte Konzepte

Benutzer einrichten
E-Mail-Unterstützung und angepasste E-Mail-Benachrichtigungen

Verwandte Verfahrensweisen

Gruppen einrichten
Administrative Konten reaktivieren
Serveradministrations-Tool öffnen

Eine Verschlüsselungsstufe festlegen

Die Verschlüsselung schützt Dateien und andere Projektinformationen vor dem Zugriff durch unautorisierte Dritte über ungeschützte Netzwerkverbindungen, z. B. über das Internet. Für die TCP/IP-Verbindungen einer Serverkonfiguration können Sie eine minimale Verschlüsselungsstufe für die IP-Adressen festlegen, die auf die Serverkonfiguration zugreifen. Sie können unterschiedliche Verschlüsselungsstufen für eine IP-Adresse, IP-Adressbereiche oder alle IP-Adressen festlegen. Dieses Thema beschreibt beide Vorgehensweisen.

Clients können die Verschlüsselungsstufe für einzelne Workstations festlegen. Benutzer müssen mindestens die minimale Verschlüsselungsstufe verwenden, die für eine Serverkonfiguration festgelegt ist.

Hinweis: Diese Operation kann nur bei gestarteter Serverkonfiguration ausgeführt werden.

So legen Sie unabhängig von der IP-Adresse die Verschlüsselungsebene für übertragene Daten fest

1. Öffnen Sie das Serveradministrations-Tool und wählen Sie die Serverkonfiguration aus, die Sie ändern möchten.

   Hinweis: Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.

2. Klicken Sie auf die Verknüpfung **Server konfigurieren** im Verknüpfungsfenster oder wählen Sie im Hauptmenü **Tools** ▸ **Administration** ▸ **Server konfigurieren**.

   Das Dialogfeld **Server konfigurieren** wird geöffnet.

3. Wählen Sie das Register **Protokoll**.
4. Wählen Sie im Listenfeld **TCP/IP-Verschlüsselungsstufen** die Option **Standard**.
5. Klicken Sie auf **Ändern**.

   Das Dialogfeld **Verschlüsselungstyp festlegen** wird geöffnet.

6. Wählen Sie den Verschlüsselungstyp aus, der bei der Serverkonfiguration für IP-Adressen verwendet werden soll, die in der Liste nicht angegeben sind.
7. Klicken Sie auf **OK**, um die Änderungen zu übernehmen und zum Register **Protokoll** zurückzukehren.
8. Klicken Sie auf **OK**.

So legen Sie eine andere Verschlüsselungsstufe für bestimmte Adressen oder Adressbereiche fest

1. Klicken Sie auf das Register **Protokoll** des Dialogfelds **Server konfigurieren** und klicken Sie dann auf **Hinzufügen**. Das Dialogfeld **Verschlüsselungstyp festlegen** wird geöffnet.
2. Geben Sie die IP-Startadresse in die Felder **IP-Startadresse** ein.
3. Geben Sie die IP-Endadresse in die Felder **IP-Endadresse** ein.
4. Wählen Sie den Verschlüsselungstyp aus, der bei der Serverkonfiguration für diese IP-Adressen verwendet werden soll.
5. Klicken Sie auf **OK**, um die Änderungen zu übernehmen und zum Register **Protokoll** zurückzukehren.
6. Klicken Sie auf **OK**.

Verwandte Verfahrensweisen

Serverkonfigurationsoptionen ändern

Verwandte Referenz

Optionen des Dialogfelds 'Server konfigurieren'

Server-Zeitlimit-Optionen ändern

In diesem Thema werden die folgenden Verfahrensweisen beschrieben:

- Zeitlimit beim Anmeldevorgang ändern
- Zeitlimit für Inaktivität ändern
- Zeitlimit für Neuverbindung ändern

So ändern Sie das Zeitlimit beim Anmeldevorgang

1. Öffnen Sie das Serveradministrations-Tool und wählen Sie die Serverkonfiguration aus, die Sie ändern möchten.

   Hinweis: Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.

2. Klicken Sie auf die Verknüpfung **Server konfigurieren** im Verknüpfungsfenster oder wählen Sie **Tools** ▸ **Administration** ▸ **Server konfigurieren** im Hauptmenü.

   Das Dialogfeld **Server konfigurieren** wird geöffnet.

3. Klicken Sie auf das Register **Allgemein**.
4. Geben Sie in das Textfeld **Zeitlimit beim Anmeldevorgang** die Anzahl der **Sekunden** ein, die Benutzern für die Anmeldung zur Verfügung stehen sollen.

   Das Zeitlimit für die Anmeldung beträgt fünf Minuten.

5. Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

Hinweis: Diese Option steht nur bei einer gestarteten Serverkonfiguration zur Verfügung.

So legen Sie das Zeitlimit für Inaktivität für Benutzer fest

1. Öffnen Sie das Serveradministrations-Tool und wählen Sie die Serverkonfiguration aus, die Sie ändern möchten.

   Hinweis: Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.

2. Klicken Sie auf die Verknüpfung **Server konfigurieren** im Verknüpfungsfenster oder wählen Sie **Tools** ▸ **Administration** ▸ **Server konfigurieren** im Hauptmenü.

   Das Dialogfeld **Server konfigurieren** wird geöffnet.

3. Klicken Sie auf das Register **Allgemein**.
4. Aktivieren Sie das Auswahlfeld **Zeitlimit für Inaktivität** .
5. Geben Sie in das Textfeld **Zeitlimit für Inaktivität** die Anzahl der Minuten ein. Klicken Sie auf "OK".
6. Optional können Sie die Option **Benannte Benutzer ausschließen** aktivieren, damit benannte Benutzer (Benutzer mit einer personengebundenen Lizenz) auch dann angemeldet bleiben können, wenn sie das **Zeitlimit für Inaktivität** überschreiten.
7. Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

Hinweis: Diese Optionen stehen nur bei einer gestarteten Serverkonfiguration zur Verfügung.

So ändern Sie das Zeitlimit für Neuverbindungen

1 Öffnen Sie das Serveradministrations-Tool und wählen Sie die Serverkonfiguration aus, die Sie ändern möchten.

Hinweis: Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.

2 Klicken Sie im Verknüpfungsfenster auf die Verknüpfung **Server konfigurieren** oder wählen Sie **Tools ▸ Administration ▸ Server konfigurieren** im Hauptmenü. Das Dialogfeld **Server konfigurieren** wird geöffnet.

3 Klicken Sie auf das Register **Allgemein**.

4 Aktivieren Sie das Auswahlfeld **Zeitlimit für Neuverbindung**.

5 Geben Sie eine Anzahl von Minuten in das Textfeld ein, um den Wert für das Zeitlimit für die Neuverbindung festzulegen. Der Standardwert ist 30 Minuten.

6 Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

Verwandte Konzepte

Server-Zeitlimit-Optionen

Verwandte Verfahrensweisen

Serveradministrations-Tool öffnen
Serverkonfigurationsoptionen ändern

Verwandte Referenz

Optionen des Dialogfelds 'Server konfigurieren'

Server migrieren

Dieser Abschnitt beschreibt Verfahrensweisen zum Migrieren von Daten zwischen zwei Servern.

In diesem Abschnitt

Serverkonfigurationen auf einen neuen Server verschieben

Dieses Thema enthält Folgendes:

- Schritte vor dem Migrieren einer Serverkonfiguration
- Serverkonfiguration migrieren
- Schritte nach dem Migrieren einer Serverkonfiguration

So bereiten Sie die Migration einer Serverkonfiguration vor

1. Fahren Sie die Serverkonfiguration herunter.
2. Erstellen Sie ein Backup der Datenbank.
3. Überprüfen Sie den Speicherort der zu verschiebenden Dateien. Dabei handelt es sich um folgende Dateien:
   - Das Datenbank-Backup
   - `starteam-server-configs.xml`
   - Das Repository einschließlich seiner Native-II-Archive, sofern sich diese nicht unter dem Repository-Ordner befinden.

So migrieren Sie eine Serverkonfiguration

1. Kopieren Sie die Dateien vom Quell- an den Zielspeicherort.
2. Öffnen Sie die Datei `starteam-server-configs-xml` in einem Texteditor.
3. Kopieren Sie die gesamte Quell-Serverkonfiguration in die Zieldatei `starteam-server-configs-xml` .

   Hinweis: Wenn die Datei `starteam-server-configs-xml` auf dem Zielcomputer nicht vorhanden ist, kopieren Sie die gesamte Datei und löschen Sie alle Einträge aus der Datei für Serverkonfigurationen, die auf dem Zielcomputer nicht vorhanden sind. Wenn diese Datei jedoch auf dem Zielcomputer vorhanden ist, achten Sie darauf, dass Sie nur den Abschnitt kopieren, der für die Serverkonfiguration erforderlich ist, die Sie auf den Zielcomputer verschieben.

4. Öffnen Sie die Datei `starteam-server-configs-xml`.
5. Geben Sie für die migrierte Serverkonfiguration die richtigen Werte unter den Optionen `RepositoryPath` und `LogPath` ein, sodass sie auf die neuen migrierten Speicherorte für die angegebene Serverkonfiguration verweisen.

   Sie würden die Werte dieser Optionen beispielsweise wie folgt aktualisieren:

   - `<Optionsname="RepositoryPath" Wert="C:\Programme\Borland\StarTeam Server 2009\Samples\StarDraw Repository\" />`
   - `<option name="LogPath" value="C:\Programme\Borland\StarTeam Server 2009 \Samples\StarDraw Repository\" />`

So schließen Sie die Migration einer Serverkonfiguration ab

1. Stellen Sie die Datenbank aus dem Backup wieder her.
2. Konfigurieren Sie eine ODBC-Verbindung für die migrierte Serverkonfiguration.
3. Starten Sie die migrierte Serverkonfiguration. Abhängig davon, ob auf demselben Server weitere Serverkonfigurationen ausgeführt werden, müssen Sie die migrierte Serverkonfiguration auf einem anderen Port starten. Wenn dies erforderlich ist, führen Sie einen der folgenden Schritte aus:
    - Klicken Sie auf die Schaltfläche **Mit angepassten Serveroptionen starten** in der Symbolleiste oder
    - wählen Sie im Hauptmenü **Aktionen** ▸ **Mit angepassten Serveroptionen starten**.

Verwandte Konzepte

Backups
Speicherorte für die Datenspeicherung

Verwandte Verfahrensweisen

Informationen sichern
Server migrieren
Serverkonfigurationen starten und stoppen
Optionen für die Datenspeicherung konfigurieren

Serverkonfigurationen in andere Datenbanken migrieren

Mit dem Dienstprogramm Serveradministrations-Tool können Sie alle vom Server unterstützten Datenbanken miteinander migrieren. Beispielsweise können Sie mit dieser Funktion eine Oracle-Datenbank in eine Microsoft SQL Server-Datenbank migrieren. Durch die Migrationsfunktion werden Informationen über die neue Serverkonfiguration zur Datei `starteam-server-configs.xml` hinzugefügt.

Dieses Thema enthält Folgendes:

- Schritte vor dem Migrieren einer Datenbank
- Datenbanken migrieren
- Schritte nach dem Migrieren einer Datenbank

Hinweis: Diese Operation kann nur bei deaktivierter Serverkonfiguration ausgeführt werden.

So bereiten Sie das Migrieren einer Datenbank vor

1. Erstellen Sie ein Backup der zu migrierenden Datenbank. Stellen Sie außerdem sicher, dass Sie über Backups der Dateien und Ordner des Serverkonfigurations-Repositorys verfügen.
2. Stellen Sie sicher, dass die zu migrierende Datenbank unbeschädigt ist. Gehen Sie dazu wie folgt vor:
   - Führen Sie Vault Verify aus.
   - Aktivieren Sie ein Verifizierungs-Tool Ihres Datenbankherstellers.
3. Führen Sie einen der folgenden Schritte aus:
   - Erstellen Sie manuell einen Datenbank- oder Schema-Benutzer als Empfänger der migrierten Daten. Weitere Informationen hierzu finden Sie im StarTeam-Installationshandbuch *StarTeam installieren* (`install_de.pdf`). Stellen Sie sicher, dass Sie sich den DNS-Namen, den Benutzernamen und das Passwort für den Datenbank- bzw. Schema-Benutzer notieren. Dieser Benutzer muss mindestens über die Berechtigung zum Erstellen von Tabellen und gespeicherten Prozeduren verfügen (wenn die Datenbank gespeicherte Prozeduren unterstützt).
   - Erstellen Sie mit dem Serveradministrations-Tool automatisch einen Datenbank- oder Schema-Benutzer als Empfänger der migrierten Daten.
4. Planen Sie die Datenbankmigration für einen Zeitpunkt, zu dem möglichst wenig Benutzer davon betroffen sind. Eine Serverkonfiguration kann nicht aktiv sein, während die Datenbank migriert wird.

   Benachrichtigen Sie Ihre Teammitglieder im Voraus über die geplante Migration, teilen Sie Ihnen den Zeitpunkt der Migration mit und fordern Sie diese auf, ihre Dateien einzuchecken.

So migrieren Sie eine Datenbank

1. Öffnen Sie das Serveradministrations-Tool und wählen Sie im Serverfenster die gewünschte Serverkonfiguration aus.

   Hinweis: Die Serverkonfiguration darf während der Datenbankmigration nicht aktiv sein.
2. Klicken Sie auf den Symbolleistenschalter **Datenbank migrieren** oder wählen Sie im Hauptmenü **Aktionen ▸ Migrieren**. Sie werden gewarnt, dass Sie Serverkonfigurationen nur migrieren können, wenn der Server registriert ist.

Hinweis: Weitere Informationen darüber, wie Sie den Server registrieren (Lizenzdaten hinzufügen), finden Sie unter dem Link "Native Lizenzen verwenden" am Ende dieses Themas.

3 Wenn der Server registriert ist, klicken Sie auf **Ja**. Der Experte **Neue Zielkonfiguration für die Migration erstellen** wird geöffnet.

4 Führen Sie auf der ersten Seite des Experten (**Zielkonfiguration für Migration auswählen**) folgende Schritte aus:

   1 Geben Sie den Namen der neuen Serverkonfiguration in das Textfeld **Konfigurationsname** unter "Ziel" ein.

   2 Klicken Sie auf **Weiter**. Die zweite Seite des Experten (**Neue Konfigurationsdaten eingeben**) wird geöffnet.

5 Geben Sie im Dropdown-Listenfeld **Datenbanktyp** den Typ der Datenbank an.

6 Führen Sie einen der folgenden Schritte aus:

- *(Empfohlene Standardaktion)* Aktivieren Sie **Neue StarTeam-Datenbank und ODBC-Datenquelle erstellen**.
- Deaktivieren Sie das Auswahlfeld, wenn Sie für diese Migration bereits manuell einen Datenbank- oder Schema-Benutzer erstellt haben.

7 Klicken Sie auf **Weiter**, wenn Sie alle Informationen eingegeben haben.

Ab diesem Schritt sind die Dialogfelder identisch mit den Dialogfeldern, die beim Erstellen einer Serverkonfiguration angezeigt werden.

So schließen Sie die Datenbankmigration ab

1 Deaktivieren Sie die alte Serverkonfiguration. So verhindern Sie, dass diese unabsichtlich gestartet wird und jemand auf sie zugreift.

   1 Wählen Sie die alte Serverkonfiguration im Serveradministrations-Tool aus.

   2 Klicken Sie auf den Symbolleistenschalter **Server deaktivieren** oder wählen Sie im Hauptmenü **Aktionen ▸ Server aktivieren**. Das Statussymbol links neben dem Namen der Serverkonfiguration ändert sich in das Symbol *Deaktiviert*.

Tipp: Weitere Informationen zur Liste der Statussymbole für Serverkonfigurationen finden Sie unter dem Link "Symbole für den Serverkonfigurationsstatus" am Ende dieses Themas.

Warnung: Die alte und die neue Serverkonfiguration greifen auf dieselben Ordner für den Datenspeicher, den Cache und die Anhänge zu. Sie greifen allerdings nicht auf dieselbe Datenbank zu. Wenn Sie die alte Serverkonfiguration weiterhin verwenden, erhalten Sie Fehlermeldungen bei der Datenspeicher-Verifizierung. Dies muss vermieden werden.

2 Leeren Sie den *Cache*-Ordner des Hives, bevor Sie die neue Serverkonfiguration starten. Der *Cache*-Ordner befindet sich standardmäßig als untergeordneter Ordner des Hives im Stammordner des Repositorys.

3 Nachdem Sie getestet haben, dass die neue Konfiguration ordnungsgemäß funktioniert, löschen Sie Folgendes:

- Die alte Serverkonfiguration

- Die von dieser Konfiguration verwendete Datenbank und
- den System-DSN.

4 (Optional) Die Tabelle *Z99* ist eine temporäre Tabelle, in der der Fortschritt der Datenbankmigration aufgezeichnet wird. Wenn der Migrationsvorgang vor der Fertigstellung abgebrochen wird, verwendet er die Tabelle *Z99*, um zu ermitteln, an welcher Stelle die Migration wieder aufgenommen werden soll, wenn der Vorgang erneut gestartet wird. Wenn der Migrationsprozess nicht ordnungsgemäß abgeschlossen wurde, können Sie die folgenden Spalten prüfen, um zu ermitteln, wie weit der Migrationsprozess fortgeschritten ist.

- Spalte 1 enthält den Namen der Quelltabelle.
- Spalte 2 enthält die ID der letzten Datensatzkopie.
- Spalte 4 enthält entweder ein "Y" oder ein "N", um anzugeben, ob eine Tabelle vollständig kopiert wurde.

Verwandte Konzepte

Backups
Speicherorte für die Datenspeicherung

Verwandte Verfahrensweisen

Dateirevisionen mit Vault Verify verifizieren
Informationen sichern
Native Lizenzen verwenden
Optionen für die Datenspeicherung konfigurieren

Verwandte Referenz

Symbole für den Serverkonfigurationsstatus

Benutzer und Gruppen verwalten

Dieser Abschnitt beschreibt Vorgehensweisen zum Verwalten von Benutzern und Gruppen.

In diesem Abschnitt

Abmelden von Benutzern erzwingen

Es kann eine Reihe von Gründen geben, die es erforderlich machen, das Abmelden von Benutzern zu erzwingen, z. B. Code-Verletzungen oder die Systemwiederherstellung nach einem Absturz. Wenn Sie die Abmeldung eines Benutzers erzwingen, wird bei der nächsten Operation des Benutzers die folgende Fehlermeldung angezeigt:`Sie sind nicht mehr angemeldet.`

Je nach dem Grund für Ihr Handeln müssen Sie den Benutzer mithilfe einer weiteren Methode, z. B. per E-Mail oder Telefon, darüber in Kenntnis setzen, dass er nicht mehr auf die Anwendung zugreifen kann.

Um sich erneut anzumelden, muss der Benutzer die Anwendung verlassen und anschließend neu starten. Die meisten Integrationen zwischen StarTeam und anderen Anwendungen erfordern einen Neustart der jeweiligen Anwendung. Die Benutzer dieser Anwendungen werden jedoch in der Regel nicht darüber informiert, dass ihre Verbindungen mit dem Server beendet wurden. Diese Operation kann nur bei aktiviertem Server ausgeführt werden.

So erzwingen Sie das Abmelden eines Benutzers

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.
2. Wählen Sie in der Serverliste eine Serverkonfiguration aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.
3. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie im unteren linken Fenster auf **Konten**. Klicken Sie anschließend auf die Verknüpfung **Benutzer-Manager**.
   - Wählen Sie im Menü **Tools** ▸ **Konten** ▸ **Benutzer-Manager**.

   Das Dialogfeld **Benutzer-Manager** wird angezeigt.
4. Wählen Sie den Benutzer aus. Wenn der gewünschte Benutzername nicht im Listenfeld **Benutzer** angezeigt wird, können Sie eine Liste aller Benutzer anzeigen, indem Sie folgende Schritte ausführen:
   1. Wählen Sie in der Baumstruktur **Gruppen** die Gruppe **All Users**.
   2. Aktivieren Sie das Auswahlfeld **Benutzer in allen nachfolgenden Gruppen anzeigen**.
5. Klicken Sie mit der rechten Maustaste auf den Benutzernamen und wählen Sie im Kontextmenü die Option **Abmeldung erzwingen**. Dem Benutzer wird der Zugriff auf die Serverkonfiguration und alle Projekte darin direkt verweigert.

   Hinweis: Sie können Ihre eigene Abmeldung nicht erzwingen.

Verwandte Konzepte

Benutzer einrichten

Verwandte Verfahrensweisen

Gruppen einrichten
Administrative Konten reaktivieren
Anzahl der möglichen Anmeldeversuche konfigurieren
Serveradministrations-Tool öffnen

Administrative Konten reaktivieren

Jedes Benutzerkonto, auch das eines Administrators, kann für eine Serverkonfiguration gesperrt werden, wenn die Anzahl der Anmeldeversuche mit einem falschen Passwort überschritten wird. Die Sperrzeit für das Hauptverwaltungskonto (Administrator) beträgt 24 Stunden. Sie können die Sperre des administrativen Kontos jedoch vor Ablauf der 24 Stunden aufheben, indem Sie wie folgt vorgehen:

So heben Sie die Sperre des Administratorkontos auf

1. Fahren Sie die Serverkonfiguration herunter und trennen Sie die Verbindung zum Netzwerk, um Remote-Benutzern den Zugriff auf die Serverkonfiguration zu verweigern.
2. Starten Sie die Serverkonfiguration vom Installationsordner des Servers aus über die Befehlszeile im Vordergrund.

   Beispiel: `starteamserver -start StarDraw -fg`

   Bei der Eingabe des Konfigurationsnamens muss die Groß-/Kleinschreibung beachtet werden. Die Eingabeaufforderung darf erst geschlossen werden, wenn die Serverkonfiguration heruntergefahren wurde.
3. Setzen Sie die Systemuhr einen Tag herauf.
4. Melden Sie sich als Administrator an und wieder ab. Das Administratorkonto wird reaktiviert.
5. Setzen Sie die Uhrzeit wieder um einen Tag auf die ursprüngliche Zeit zurück.
6. Fahren Sie die Serverkonfiguration herunter, indem Sie "X" eingeben und auf "Type" klicken. (Herunterfahren des Servers im Vordergrund)

Verwandte Verfahrensweisen

Gruppen einrichten
Benutzer einrichten
Abmelden von Benutzern erzwingen
Anzahl der möglichen Anmeldeversuche konfigurieren

Anzahl der möglichen Anmeldeversuche konfigurieren

Sie können die Sicherheit Ihrer Projekte erhöhen, indem Sie Einstellungen für Anmeldefehler und Zeitlimits für Anmeldevorgänge festlegen. Eine Ursache für Anmeldefehler kann sein, dass Hacker versuchen, Benutzerpasswörter auszuspionieren. In solchen Fällen sollten Sie die IP-Adresse des Systems möglicherweise ändern, um es den Angreifern zu erschweren, die Serverkonfiguration zu finden und ihre Angriffe zu wiederholen. Gegebenenfalls sollten Sie auch die Benutzernamen aller Benutzer des Systems ändern.

Sie können die Serverkonfiguration so konfigurieren, dass Mitglieder der Gruppe "Security Administrators" per E-Mail über fehlgeschlagene Anmeldungen benachrichtigt werden.

Hinweis: Diese Operation kann nur bei aktiviertem Server ausgeführt werden.

So legen Sie ein Limit für Anmeldeversuche fest

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.
2. Wählen Sie in der Serverliste eine Serverkonfiguration aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.
3. Wählen Sie im Hauptmenü **Tools** ▸ **Konten** ▸ **Systemrichtlinie**. Das Dialogfeld **Systemrichtlinie** wird geöffnet.
4. Wählen Sie das Register **Fehler bei der Anmeldung**.
5. Wählen Sie eine der folgenden Optionen für **Fehlschläge bei der Anmeldung** aus:
   - **Ignorieren**: Fehler bei der Anmeldung werden nicht berücksichtigt.
   - **Konto sperren nach ___ Fehlschlägen**: Geben Sie die Anzahl der zulässigen Fehlschläge bei der Anmeldung ein.
6. Wählen Sie eine der folgenden Option unter **Sperrdauer** aus:
   - **Dauerhaft**: Wenn diese Option ausgewählt ist, kann nur der Administrator die Sperre für den Benutzer aufheben.
   - **Sperre beibehalten für ___ Minuten**: Geben Sie an, wie viele Minuten die Sperre andauern soll. Nach der angegebenen Sperrfrist kann sich der Benutzer erneut anmelden.
7. Um Mitglieder der Gruppe "Security Administrators" über StarTeam-Benutzer zu informieren, deren Anmeldung nicht erfolgreich war, aktivieren Sie das Auswahlfeld **Per E-Mail**.
8. Klicken Sie auf **OK**, um die Änderungen zu übernehmen und das Dialogfeld zu schließen.

Verwandte Konzepte

Benutzer einrichten
E-Mail-Unterstützung und angepasste E-Mail-Benachrichtigungen

Verwandte Verfahrensweisen

Gruppen einrichten
Administrative Konten reaktivieren
Serveradministrations-Tool öffnen

Benutzer einrichten

Wenn Sie über die erforderlichen Zugriffsrechte verfügen, können Sie Benutzer über das Dienstprogramm "Serveradministration" oder über einen Client zur Serverkonfiguration hinzufügen. Benutzer werden zunächst zu einer bestimmten Gruppe hinzugefügt, z. B. "Developers" oder "Testers". Die Benutzer werden explizite Mitglieder dieser Gruppe und implizite Mitglieder aller übergeordneten Gruppen dieser Gruppe, beispielsweise der Gruppe "All Users". Diese Operation kann nur bei aktiviertem Server ausgeführt werden.

Warnung: Das Erstellen eines Benutzerkontos mit dem Namen "StarTeam" kann möglicherweise zu Problemen führen, wenn von der Befehlszeile aus der Servermodus-Befehl `stcmd` ausgeführt wird, um die Serverkonfiguration zu sperren oder zu entsperren. Der Befehl beinhaltet eine Passwortabfrage, selbst wenn der Benutzer über ein leeres Passwort verfügt oder wenn das Passwort bereits eingegeben wurde.

So fügen Sie einen Benutzer hinzu

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool.

   Hinweis: Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.

2. Wählen Sie in der Serverliste eine Serverkonfiguration aus.

   Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.

3. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie auf die Leiste **Konten** im unteren linken Fenster und dann auf die Verknüpfung **Benutzer-Manager**.
   - Wählen Sie im Menü **Tools** ▶ **Konten** ▶ **Benutzer-Manager**.

   Das Dialogfeld **Benutzer-Manager** wird angezeigt.

4. Wählen Sie aus der Baumstruktur **Gruppen** eine Gruppe aus und klicken Sie auf **Neuer Benutzer**. Das Dialogfeld **Eigenschaften für den neuen Benutzer** wird angezeigt.
5. Geben Sie den Namen des Benutzers in das Textfeld **Vollständiger Name** und optional die E-Mail-Adresse des Benutzers in das Textfeld **E-Mail** ein.
6. Geben Sie optional die Telefonnummer, Voice-Mail-Nummer, Pager-Nummer, Faxnummer und Anschrift des Benutzers in die entsprechenden Textfelder ein.
7. Wählen Sie das Register **Anmeldung**.

   1. Geben Sie den Namen, der zum Anmelden bei der Anwendung verwendet wird, in das Textfeld **Benutzername** ein. Wenn Sie einen bereits vorhandenen Benutzernamen eingeben, wird folgende Meldung angezeigt, nachdem Sie auf "OK" geklickt haben:`Ein Benutzer mit dem angegebenen Benutzernamen ist bereits vorhanden.`
   2. Wählen Sie den Schalter **Über StarTeam-Server validieren**, wenn Sie den Benutzer mithilfe des Servers überprüfen möchten. Geben Sie ein StarTeam-Passwort für den Benutzer in das Textfeld **Passwort** und erneut in das Textfeld **Bestätigung** ein. In dem Textfeld werden Sternchen anstelle des Passworts angezeigt. Falls die minimale Länge für das Passwort 0 ist, müssen Sie kein Passwort eingeben. Falls Sie sichere Passwörter verwenden, müssen Sie die Regeln für derartige Passwörter befolgen.
   3. (Nur Microsoft Active Directory oder OpenLDAP) Wenn Sie den Benutzer mithilfe des Verzeichnisservers der Organisation validieren möchten, wählen Sie den Schalter **Über Verzeichnisdienst validieren** und geben Sie den **eindeutigen Namen** für den Benutzer ein. Dies ist ein alphanumerischer Wert mit bis zu 254 Zeichen, der als eindeutige Identifikation des Verzeichnisdienstbenutzers verwendet wird. Damit

Benutzer die Validierung durch den Verzeichnisdienst ausführen lassen können, muss der Server in einer Domäne installiert sein, die der LDAP-Server als vertrauenswürdig erkennt.

8 Wählen Sie optional das Register **Zugriffsrichtlinie** und geben Sie an, wann dieser Benutzer auf die Serverkonfiguration zugreifen kann. Wählen Sie einen der folgenden Optionsschalter:

- Zugriff nicht beschränkt - Der Benutzer kann jederzeit auf die Serverkonfiguration zugreifen.
- Normale Fünf-Tage-Arbeitswoche (8 - 17 Uhr) - Der Benutzer kann von Montag bis Freitag zwischen 8 und 17 Uhr auf die Serverkonfiguration zugreifen.
- Angepasste Zugriffsstunden - Es werden bis zu zwei Zeiträume pro Tag festgelegt, in denen dem Benutzer der Zugriff auf die Serverkonfiguration gewährt oder verweigert wird.
- Wählen Sie im Listenfeld "Tag" einen Wochentag aus.
- Aktivieren bzw. deaktivieren Sie das Auswahlfeld "Kein Zugriff an diesem Tag", wenn an dem Tag der Zugriff verweigert bzw. gewährt werden soll.
- Verwenden Sie die Felder "Von" und "Bis", um bis zu zwei Zeiträume einzustellen, in denen der Zugriff entweder erlaubt oder verweigert wird.

Wenn sich die Workstation des Benutzers nicht in derselben Zeitzone befindet wie der Computer, auf dem die Serverkonfiguration läuft, aktivieren Sie das Auswahlfeld **An Workstation-Zeitzone anpassen** und geben Sie in das Feld **Zeitunterschied zu GMT** die Abweichung von der Greenwich Mean Time (GMT) in Stunden ein.

9 Fügen Sie den neuen Benutzer ggf. explizit in anderen Gruppen hinzu. Beachten Sie, dass ein Benutzer bereits implizit Mitglied der übergeordneten Gruppe der aktuellen Gruppe ist, aber explizit zu Gruppen hinzugefügt werden muss, die keine übergeordneten Gruppen der aktuellen Gruppe sind.

So zeigen Sie die expliziten Gruppenmitgliedschaften eines Benutzers an:

1 Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.

2 Wählen Sie in der Serverliste eine Serverkonfiguration aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.

3 Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf die Leiste **Konten** im unteren linken Fenster und dann auf die Verknüpfung **Benutzer-Manager**.
- Wählen Sie im Menü **Tools** ▸ **Konten** ▸ **Benutzer-Manager**.

Das Dialogfeld **Benutzer-Manager** wird angezeigt.

4 Wählen Sie den Benutzer aus.

Wenn der gewünschte Benutzername nicht im Listenfeld **Benutzer** angezeigt wird, können Sie eine Liste aller Benutzer anzeigen, indem Sie folgende Schritte ausführen:

1 Wählen Sie in der Baumstruktur **Gruppen** die Gruppe **All Users**.

2 Aktivieren Sie das Auswahlfeld **Benutzer in allen nachfolgenden Gruppen anzeigen**.

5 Klicken Sie mit der rechten Maustaste und wählen Sie im Kontextmenü die Option **Eigenschaften**. Das Dialogfeld **Benutzereigenschaften** wird angezeigt.

6 Wählen Sie das Register **Mitgliedschaft**. Im Listenfeld werden die Gruppen angezeigt, in denen der Benutzer explizit Mitglied ist.

So ändern Sie die Gruppenmitgliedschaft

1 Wählen Sie den Benutzer aus der Liste **Benutzer** im Dialogfeld **Benutzer-Manager**.
2 Klicken Sie mit der rechten Maustaste und wählen Sie im Kontextmenü die Option **Gruppenmitgliedschaft**. Das Dialogfeld **Gruppenmitgliedschaft** wird angezeigt.
3 Wählen Sie die Gruppen aus, zu denen der Benutzer explizit hinzugefügt werden soll.
4 Klicken Sie auf **OK**.

So entfernen Sie Benutzer aus Gruppen

1 Öffnen Sie das Dienstprogramm Serveradministrations-Tool.

Hinweis: Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.

2 Wählen Sie in der Serverliste eine Serverkonfiguration aus.

Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.

3 Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf die Leiste **Konten** im unteren linken Fenster und dann auf die Verknüpfung **Benutzer-Manager**.
- Wählen Sie im Menü **Tools** ▶ **Konten** ▶ **Benutzer-Manager**.

Das Dialogfeld **Benutzer-Manager** wird angezeigt.

4 Wählen Sie den Benutzer aus.

Wenn der gewünschte Benutzername nicht im Listenfeld **Benutzer** angezeigt wird, können Sie eine Liste aller Benutzer anzeigen, indem Sie folgende Schritte ausführen:

   1 Wählen Sie in der Baumstruktur **Gruppen** die Gruppe **All Users**.
   2 Aktivieren Sie das Auswahlfeld **Benutzer in allen nachfolgenden Gruppen anzeigen**.

5 Klicken Sie mit der rechten Maustaste auf den Benutzernamen und wählen Sie im Menü **Gruppenmitgliedschaft**. Das Dialogfeld **Gruppenmitgliedschaft** wird angezeigt.
6 Wählen Sie das Optionsfeld neben der Gruppe ab, aus der Sie den Benutzer entfernen möchten.
7 Klicken Sie auf **OK**.

So prüfen Sie den Kontostatus von Benutzern

1 Öffnen Sie das Dienstprogramm Serveradministrations-Tool.

Hinweis: Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.

2 Wählen Sie in der Serverliste eine Serverkonfiguration aus.

Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.

3 Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf die Leiste **Konten** im unteren linken Fenster und dann auf die Verknüpfung **Benutzer-Manager**.

- Wählen Sie im Menü **Tools** ▸ **Konten** ▸ **Benutzer-Manager**.

Das Dialogfeld **Benutzer-Manager** wird angezeigt.

4 Wählen Sie in der Baumstruktur **Gruppen** die Gruppe **All Users**.

5 Aktivieren Sie das Auswahlfeld **Benutzer in allen nachfolgenden Gruppen anzeigen**.

6 Prüfen Sie die Informationen eines Benutzers, der im Listenfeld **Benutzer** angezeigt wird.

Tipp: Um sicherzustellen, dass die Informationen im Listenfeld "Benutzer" aktuell sind, klicken Sie auf **Aktualisieren**.

So entfernen Sie Benutzerkonten

1 Öffnen Sie das Dienstprogramm Serveradministrations-Tool.

Hinweis: Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.

2 Wählen Sie in der Serverliste eine Serverkonfiguration aus.

Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.

3 Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf die Leiste **Konten** im unteren linken Fenster und dann auf die Verknüpfung **Benutzer-Manager**.
- Wählen Sie im Menü **Tools** ▸ **Konten** ▸ **Benutzer-Manager**.

Das Dialogfeld **Benutzer-Manager** wird angezeigt.

4 Wählen Sie den Benutzer aus. Wenn der gewünschte Benutzername nicht im Listenfeld **Benutzer** angezeigt wird, können Sie eine Liste aller Benutzer anzeigen, indem Sie folgende Schritte ausführen:

   1 Wählen Sie in der Baumstruktur **Gruppen** die Gruppe **All Users**.

   2 Aktivieren Sie das Auswahlfeld **Benutzer in allen nachfolgenden Gruppen anzeigen**.

5 Klicken Sie mit der rechten Maustaste auf den Benutzernamen und wählen Sie im Kontextmenü die Option **Konto löschen**.

Das System zeigt die folgende Meldung an:

```
Möchten Sie das Benutzerkonto "Benutzername" löschen?
```

6 Klicken Sie auf **Ja**.

Der Benutzer wird dauerhaft aus der Serverkonfiguration entfernt.

So sperren Sie Benutzerkonten vorübergehend

1 Öffnen Sie das Dienstprogramm Serveradministrations-Tool.

Hinweis: Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.

2 Wählen Sie in der Serverliste eine Serverkonfiguration aus.

Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.

3 Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf die Leiste **Konten** im unteren linken Fenster und dann auf die Verknüpfung **Benutzer-Manager**.
- Wählen Sie im Menü **Tools** ▸ **Konten** ▸ **Benutzer-Manager**.

Das Dialogfeld **Benutzer-Manager** wird angezeigt.

4 Wählen Sie den Benutzer aus.

Wenn der gewünschte Benutzername nicht im Listenfeld **Benutzer** angezeigt wird, können Sie eine Liste aller Benutzer anzeigen, indem Sie folgende Schritte ausführen:

1 Wählen Sie in der Baumstruktur **Gruppen** die Gruppe **All Users**.

2 Aktivieren Sie das Auswahlfeld **Benutzer in allen nachfolgenden Gruppen anzeigen**.

5 Klicken Sie mit der rechten Maustaste auf den Benutzernamen und wählen Sie im Kontextmenü die Option **Konto sperren**. Der Kontostatus im Listenfeld "Benutzer" ändert sich in "Deaktiviert" und der Zugriff auf den Server wird nach der Abmeldung des Benutzers verweigert.

Hinweis: Sie können Ihr eigenes Benutzerkonto nicht sperren.

So aktivieren Sie Benutzerkonten wieder

1 Öffnen Sie das Dienstprogramm Serveradministrations-Tool.

Hinweis: Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.

2 Wählen Sie in der Serverliste eine Serverkonfiguration aus.

Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.

3 Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf die Leiste **Konten** im unteren linken Fenster und dann auf die Verknüpfung **Benutzer-Manager**.
- Wählen Sie im Menü **Tools** ▸ **Konten** ▸ **Benutzer-Manager**.

Das Dialogfeld **Benutzer-Manager** wird angezeigt.

4 Wählen Sie den Benutzer aus.

Wenn der gewünschte Benutzername nicht im Listenfeld **Benutzer** angezeigt wird, können Sie eine Liste aller Benutzer anzeigen, indem Sie folgende Schritte ausführen:

1 Wählen Sie in der Baumstruktur **Gruppen** die Gruppe **All Users**.

2 Aktivieren Sie das Auswahlfeld **Benutzer in allen nachfolgenden Gruppen anzeigen**.

5 Klicken Sie mit der rechten Maustaste auf den Benutzernamen und wählen Sie im Kontextmenü die Option **Konto reaktivieren**. Das Benutzerkonto wird reaktiviert.

Verwandte Konzepte

Übersicht über Benutzer- und Gruppenkonfigurationen

Verwandte Verfahrensweisen

Serveradministrations-Tool öffnen

Benutzerpasswörter ändern

Zusätzlich zum Einrichten oder Ändern eines Benutzerpassworts können Sie angeben, wie lange ein Passwort gültig ist, wie viele Zeichen es mindestens haben muss und ob sichere Passwörter erforderlich sind. Diese Operation kann nur bei aktiviertem Server ausgeführt werden.

So ändern Sie ein Passwort:

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.
2. Wählen Sie in der Serverliste eine Serverkonfiguration aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.
3. Wählen Sie im Menü **Tools** ▸ **Konten** ▸ **Benutzer-Manager**. Dadurch wird das Dialogfeld "Benutzer-Manager" angezeigt.
4. Wählen Sie den Benutzernamen aus. Wenn der gewünschte Benutzername nicht im Listenfeld "Benutzer" angezeigt wird, können Sie eine Liste aller Benutzer anzeigen, indem Sie das Auswahlfeld **Benutzer in allen nachfolgenden Gruppen anzeigen** aktivieren.
5. Klicken Sie mit der rechten Maustaste und wählen Sie im Kontextmenü die Option "Eigenschaften". Das Dialogfeld **Benutzereigenschaften** wird angezeigt.
6. Wählen Sie das Register **Anmeldung**.
7. Stellen Sie sicher, dass der Schalter **Über StarTeam-Server validieren** ausgewählt ist.
8. Geben Sie in das Textfeld **Passwort** ein neues StarTeam-Passwort für den Benutzer ein.
9. Geben Sie das Passwort erneut in das Textfeld **Bestätigung** ein und klicken Sie auf **OK**.

Verwandte Verfahrensweisen

Passwortänderung erzwingen
Passworteinschränkungen konfigurieren
Serveradministrations-Tool öffnen

Gruppen einrichten

Benutzer mit Zugriffsberechtigungen für eine Serverkonfiguration können in Gruppen organisiert werden. Das Erstellen und Verwenden von Gruppen vereinfacht die Sicherheitsverwaltung für ein Projekt, da jeder Gruppe eine Reihe von Berechtigungen zugewiesen werden können, die für alle Benutzer in der Gruppe gelten. Auf diese Weise vermeiden Sie es, die Berechtigungen jedem Benutzer einzeln zuweisen zu müssen.

Die Statusleiste im Dialogfeld Benutzer-Manager zeigt Folgendes an: die Anzahl der Benutzer der ausgewählten Gruppe, die über Zugriffsrechte auf die Serverkonfiguration verfügen, die Anzahl der Benutzer, die mit der Serverkonfiguration verbunden sind, und die Anzahl der angemeldeten Benutzer. Die Zahl der mit der Serverkonfiguration verbundenen Benutzer weicht von der Anzahl der angemeldeten Benutzer ab, wenn einzelne Benutzer mehrfach angemeldet sind.

Diese Operation kann nur bei aktiviertem Server ausgeführt werden.

So fügen Sie eine Gruppe hinzu

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.
2. Wählen Sie in der Serverliste eine Serverkonfiguration aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.
3. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie im unteren linken Fenster auf **Konten**. Klicken Sie anschließend auf die Verknüpfung **Benutzer-Manager**.
   - Wählen Sie im Menü **Tools** ▸ **Konten** ▸ **Benutzer-Manager**.

   Das Dialogfeld **Benutzer-Manager** wird angezeigt.
4. Wählen Sie in der Baumstruktur **Gruppen** eine Gruppe als übergeordnete Gruppe der neuen Gruppe aus.

   Hinweis: Es wird empfohlen, dass Sie die erste neue Gruppe zur Gruppe **All Users** hinzufügen. Nachfolgende Gruppen können zu einer beliebigen der Gruppen hinzugefügt werden, die unter der Gruppe **All Users** angezeigt werden. Fügen Sie möglichst keine neuen Gruppen zu den Administrator- und Management-Gruppen hinzu. Wenn ein Benutzer Mitglied einer Untergruppe ist, ist er implizit auch Mitglied der übergeordneten Gruppe, auch wenn sein Name in der Benutzerliste der übergeordneten Gruppe nicht angezeigt wird. Sie müssen das Auswahlfeld **Benutzer in allen nachfolgenden Gruppen anzeigen** aktivieren, um eine vollständige Liste der Mitglieder einer ausgewählten Gruppe anzuzeigen, die über Untergruppen verfügt.

5. Klicken Sie auf **Neue Gruppe**. Das Dialogfeld **Eigenschaften für die neue Gruppe** wird angezeigt.
6. Geben Sie in das Textfeld **Name** einen Namen für die Gruppe ein.
7. Geben Sie im Textfeld **Beschreibung** eine Beschreibung der Gruppe ein.
8. Wählen Sie das Register **Berechtigungen**.

   Im Register **Berechtigungen** ausgewählte Berechtigungen haben Vorrang vor allen Zugriffsrechten, die zuvor für Benutzer einer Gruppe festgelegt wurden. Berechtigungen sollten jedoch nicht als Ersatz für Zugriffsrechte verwendet werden. Wenn Sie keine Zugriffsrechte festgelegt haben, verfügen Sie über kein Sicherheitssystem.

   Die im Register **Berechtigungen** festgelegten Berechtigungen gelten für alle Objekte in allen Projekten einer Serverkonfiguration. Wenn Sie einer Gruppe beispielsweise die Berechtigung zum Löschen von Elementen zuweisen, können die Benutzer der Gruppe alle Projekte, Ansichten, Ordner, Unterordner oder Elemente der Serverkonfiguration löschen, unabhängig davon, welche Zugriffsrechte für das Löschen dieser Elemente definiert wurden.

9 Legen Sie die Berechtigungen wie gewünscht fest und klicken Sie auf **OK**. Die neue Gruppe wird in der Liste **Gruppen** angezeigt.

So ändern Sie eine übergeordnete Gruppe

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.
2. Wählen Sie in der Serverliste eine Serverkonfiguration aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.
3. Führen Sie einen der folgenden Schritte aus:
    - Klicken Sie im unteren linken Fenster auf **Konten**. Klicken Sie anschließend auf die Verknüpfung **Benutzer-Manager**.
    - Wählen Sie im Menü **Tools** ▸ **Konten** ▸ **Benutzer-Manager**.

    Das Dialogfeld **Benutzer-Manager** wird angezeigt.
4. Wählen Sie die Gruppe aus, die aus der Baumstruktur **Gruppen** verschoben werden soll.
5. Klicken Sie mit der rechten Maustaste und wählen Sie im Kontextmenü die Option **Übergeordnete Gruppe ändern**. Das Dialogfeld **Übergeordnete Gruppe ändern** wird angezeigt.
6. Wählen Sie eine neue übergeordnete Gruppe aus und klicken Sie anschließend auf **OK**.
7. Klicken Sie auf **OK**.

So ermitteln Sie die Mitglieder einer Gruppe

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.
2. Wählen Sie in der Serverliste eine Serverkonfiguration aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.
3. Führen Sie einen der folgenden Schritte aus:
    - Klicken Sie im unteren linken Fenster auf **Konten**. Klicken Sie anschließend auf die Verknüpfung **Benutzer-Manager**.
    - Wählen Sie im Menü **Tools** ▸ **Konten** ▸ **Benutzer-Manager**.

    Das Dialogfeld **Benutzer-Manager** wird angezeigt.
4. Wählen Sie die Gruppe in der Baumstruktur **Gruppen** aus. Die expliziten Mitglieder der Gruppe werden im Listenfeld **Benutzer** angezeigt.
5. Sie müssen das Auswahlfeld **Benutzer in allen nachfolgenden Gruppen anzeigen** aktivieren, um auch die impliziten Mitglieder der Gruppe im Listenfeld "Benutzer" anzuzeigen.

So entfernen Sie eine leere Gruppe:

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.
2. Wählen Sie in der Serverliste eine Serverkonfiguration aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.
3. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie im unteren linken Fenster auf **Konten**. Klicken Sie anschließend auf die Verknüpfung **Benutzer-Manager**.
- Wählen Sie im Menü **Tools** ▸ **Konten** ▸ **Benutzer-Manager**.

Das Dialogfeld **Benutzer-Manager** wird angezeigt.

4 Wählen Sie eine Gruppe in der Baumstruktur **Gruppen** aus.

5 Klicken Sie mit der rechten Maustaste, um das Kontextmenü anzuzeigen, und wählen Sie **Löschen**. Das System zeigt die folgende Meldung an:

```
Möchten Sie die Gruppe Gruppenname löschen?
```

6 Klicken Sie auf **Ja**.

- Wenn die Gruppe leer ist, wird Sie aus dem Listenfeld **Gruppen** entfernt.
- Wenn die Gruppe Benutzer enthält, wird folgende Meldung angezeigt:

```
Die Gruppe, die Sie löschen möchten, enthält Benutzerkonten. Löschen Sie bitte diese
Benutzerkonten oder verschieben Sie sie in eine andere Gruppe, bevor Sie diese Gruppe
löschen.
```

Klicken Sie auf **OK**, wenn die Meldung angezeigt wird. Löschen Sie die Benutzer aus dieser Gruppe oder verschieben Sie sie in eine andere Gruppe.

Verwandte Konzepte

Übersicht über Benutzer- und Gruppenkonfigurationen

Verwandte Verfahrensweisen

Serveradministrations-Tool öffnen

Passwortänderung erzwingen

Im Fall einer Sicherheitsverletzung in einem Projekt ist es möglicherweise notwendig, die Änderung von StarTeam-Benutzerpasswörtern zu erzwingen. Diese Operation kann nur bei aktiviertem Server ausgeführt werden. Sie können ein Zeitlimit für die Gültigkeitsdauer von Passwörtern und die Mindestlänge festlegen sowie die Verwendung von sicheren Passwörtern als erforderlich kennzeichnen. Diese Passworteigenschaften beziehen sich auf alle Benutzerkonten einer Serverkonfiguration.

So zwingen Sie Benutzer, ihre Passwörter zu ändern:

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.
2. Wählen Sie in der Serverliste eine Serverkonfiguration aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.
3. Klicken Sie im unteren linken Fenster auf **Konten**. Klicken Sie anschließend auf die Verknüpfung **Benutzer-Manager**. Das Dialogfeld **Benutzer-Manager** wird angezeigt.
4. Wählen Sie den Benutzer aus. Wenn der Benutzer, mit dem Sie arbeiten möchten, nicht im Listenfeld **Benutzer** angezeigt wird, können Sie eine Liste aller Benutzer anzeigen, indem Sie die Gruppe **All Users** aus der Baumstruktur **Gruppen** auswählen und das Auswahlfeld **Benutzer in allen nachfolgenden Gruppen anzeigen** aktivieren.
5. Klicken Sie mit der rechten Maustaste auf den Benutzernamen und wählen Sie im Kontextmenü die Option **Passwortänderung erzwingen**. In der Spalte **Kontostatus** im Listenfeld **Benutzer** wird Folgendes angezeigt: "Passwortänderung erforderlich". Der Benutzer wird bei der nächsten Anmeldung aufgefordert, das Passwort zu ändern. Wenn das Passwort nicht geändert wird, kann der Benutzer zwar auf die Serverkonfiguration und die zugehörigen Projekte zugreifen, sein Konto wird aber bei der nächsten Anmeldung gesperrt. Der Benutzer wird über eine Fehlermeldung hierüber in Kenntnis gesetzt.

Hinweis: Die Konten der Benutzer, die ihre Passwörter nicht ändern, können vom Administrator reaktiviert werden.

Verwandte Verfahrensweisen

Benutzerpasswörter ändern
Passworteinschränkungen konfigurieren
Serveradministrations-Tool öffnen

Passworteinschränkungen konfigurieren

Änderungen, die an der Passwortlänge vorgenommen werden, sind sofort wirksam, gelten aber nur für alle neuen Benutzerkonten oder neue Passwörter. Wenn Sie beispielsweise die Mindestlänge für Passwörter von acht in zehn Zeichen ändern, müssen alle neuen Benutzer Passwörter verwenden, die mindestens zehn Zeichen lang sind. Bereits vorhandene Benutzer können jedoch weiterhin ihre acht Zeichen langen Passwörter verwenden.

Änderungen, die an der Gültigkeitsdauer für Passwörter vorgenommen wurden, werden nach dem entsprechenden Zeitintervall wirksam. Wenn Sie beispielsweise die Gültigkeitsdauer für Passwörter auf dreißig Tage setzen, werden die Benutzerkonten gesperrt, wenn die entsprechenden Passwörter vor Ablauf des Zeitraums nicht geändert wurden. Benutzer werden zwei Wochen vor der Sperrung aufgefordert, das Passwort zu ändern. Standardmäßig ist die Option für die Verwendung von sicheren Passwörtern deaktiviert. Wenn die Funktion aktiviert wird, müssen Benutzer bei einer Änderung ihres jeweiligen Passworts ein sicheres Passwort angeben. Die alten "nicht sicheren" Passwörter bleiben bis zu einer solchen Passwortänderung gültig.

So richten Sie Beschränkungen für Passwörter ein

1 Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.

2 Wählen Sie in der Serverliste eine Serverkonfiguration aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.

3 Wählen Sie im Hauptmenü **Tools** ▸ **Konten** ▸ **Systemrichtlinie**.

4 Wählen Sie im Register **Passwörter** eine Option für die Gültigkeitsdauer für Passwörter:

- **Passwörter sind unbegrenzt gültig**
- **Passwörter werden ungültig nach ___ Tagen**. Bei dieser Option müssen Sie die Anzahl von Tagen eingeben, für die ein Passwort gültig ist. Die Tage werden ab dem Zeitpunkt gezählt, zu dem das Passwort erstellt wurde.

5 Aktivieren Sie das Auswahlfeld **Sichere Passwörter erforderlich**, wenn Passwörter die folgenden Kriterien erfüllen müssen:

- Neue Passwörter müssen sich von alten unterscheiden.
- Neue Passwörter müssen sich vom Benutzernamen unterscheiden.
- Neue Passwörter müssen Zeichen in Groß- und Kleinschreibung enthalten. Dabei muss jeweils mindestens ein Buchstabe des Alphabets in Groß- bzw. Kleinschreibung verwendet werden. (Maßgeblich hierfür ist das Basisalphabet mit 26 Buchstaben.)
- Neue Passwörter müssen mindestens ein nicht-alphabetisches Zeichen enthalten.

Wenn Sie dieses Auswahlfeld aktivieren, wird der Wert im Textfeld "Mindestlänge des Passworts" auf 3 gesetzt. Sie können diesen Wert erhöhen, wenn Sie möchten.

6 Geben Sie optional eine Zahl für die Mindestlänge des Passworts ein. Der Vorgabewert 0 ermöglicht die Eingabe leerer Passwörter. Die maximale Passwortlänge beträgt 32 Zeichen.

7 Klicken Sie auf **OK**.

Verwandte Verfahrensweisen

Benutzerpasswörter ändern
Passwortänderung erzwingen
Serveradministrations-Tool öffnen

Passwörter verwalten

Dieser Abschnitt beschreibt Vorgehensweisen zum Verwalten von Passwörtern.

In diesem Abschnitt

Benutzerpasswörter ändern

Zusätzlich zum Einrichten oder Ändern eines Benutzerpassworts können Sie angeben, wie lange ein Passwort gültig ist, wie viele Zeichen es mindestens haben muss und ob sichere Passwörter erforderlich sind. Diese Operation kann nur bei aktiviertem Server ausgeführt werden.

So ändern Sie ein Passwort:

1 Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.

2 Wählen Sie in der Serverliste eine Serverkonfiguration aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.

3 Wählen Sie im Menü **Tools** ▸ **Konten** ▸ **Benutzer-Manager**. Dadurch wird das Dialogfeld "Benutzer-Manager" angezeigt.

4 Wählen Sie den Benutzernamen aus. Wenn der gewünschte Benutzername nicht im Listenfeld "Benutzer" angezeigt wird, können Sie eine Liste aller Benutzer anzeigen, indem Sie das Auswahlfeld **Benutzer in allen nachfolgenden Gruppen anzeigen** aktivieren.

5 Klicken Sie mit der rechten Maustaste und wählen Sie im Kontextmenü die Option "Eigenschaften". Das Dialogfeld **Benutzereigenschaften** wird angezeigt.

6 Wählen Sie das Register **Anmeldung**.

7 Stellen Sie sicher, dass der Schalter **Über StarTeam-Server validieren** ausgewählt ist.

8 Geben Sie in das Textfeld **Passwort** ein neues StarTeam-Passwort für den Benutzer ein.

9 Geben Sie das Passwort erneut in das Textfeld **Bestätigung** ein und klicken Sie auf **OK**.

Verwandte Verfahrensweisen

Passwortänderung erzwingen
Passworteinschränkungen konfigurieren
Serveradministrations-Tool öffnen

Passwortänderung erzwingen

Im Fall einer Sicherheitsverletzung in einem Projekt ist es möglicherweise notwendig, die Änderung von StarTeam-Benutzerpasswörtern zu erzwingen. Diese Operation kann nur bei aktiviertem Server ausgeführt werden. Sie können ein Zeitlimit für die Gültigkeitsdauer von Passwörtern und die Mindestlänge festlegen sowie die Verwendung von sicheren Passwörtern als erforderlich kennzeichnen. Diese Passworteigenschaften beziehen sich auf alle Benutzerkonten einer Serverkonfiguration.

So zwingen Sie Benutzer, ihre Passwörter zu ändern:

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.
2. Wählen Sie in der Serverliste eine Serverkonfiguration aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.
3. Klicken Sie im unteren linken Fenster auf **Konten**. Klicken Sie anschließend auf die Verknüpfung **Benutzer-Manager**. Das Dialogfeld **Benutzer-Manager** wird angezeigt.
4. Wählen Sie den Benutzer aus. Wenn der Benutzer, mit dem Sie arbeiten möchten, nicht im Listenfeld **Benutzer** angezeigt wird, können Sie eine Liste aller Benutzer anzeigen, indem Sie die Gruppe **All Users** aus der Baumstruktur **Gruppen** auswählen und das Auswahlfeld **Benutzer in allen nachfolgenden Gruppen anzeigen** aktivieren.
5. Klicken Sie mit der rechten Maustaste auf den Benutzernamen und wählen Sie im Kontextmenü die Option **Passwortänderung erzwingen**. In der Spalte **Kontostatus** im Listenfeld **Benutzer** wird Folgendes angezeigt: "Passwortänderung erforderlich". Der Benutzer wird bei der nächsten Anmeldung aufgefordert, das Passwort zu ändern. Wenn das Passwort nicht geändert wird, kann der Benutzer zwar auf die Serverkonfiguration und die zugehörigen Projekte zugreifen, sein Konto wird aber bei der nächsten Anmeldung gesperrt. Der Benutzer wird über eine Fehlermeldung hierüber in Kenntnis gesetzt.

Hinweis: Die Konten der Benutzer, die ihre Passwörter nicht ändern, können vom Administrator reaktiviert werden.

Verwandte Verfahrensweisen

Benutzerpasswörter ändern
Passworteinschränkungen konfigurieren
Serveradministrations-Tool öffnen

Passworteinschränkungen konfigurieren

Änderungen, die an der Passwortlänge vorgenommen werden, sind sofort wirksam, gelten aber nur für alle neuen Benutzerkonten oder neue Passwörter. Wenn Sie beispielsweise die Mindestlänge für Passwörter von acht in zehn Zeichen ändern, müssen alle neuen Benutzer Passwörter verwenden, die mindestens zehn Zeichen lang sind. Bereits vorhandene Benutzer können jedoch weiterhin ihre acht Zeichen langen Passwörter verwenden.

Änderungen, die an der Gültigkeitsdauer für Passwörter vorgenommen wurden, werden nach dem entsprechenden Zeitintervall wirksam. Wenn Sie beispielsweise die Gültigkeitsdauer für Passwörter auf dreißig Tage setzen, werden die Benutzerkonten gesperrt, wenn die entsprechenden Passwörter vor Ablauf des Zeitraums nicht geändert wurden. Benutzer werden zwei Wochen vor der Sperrung aufgefordert, das Passwort zu ändern. Standardmäßig ist die Option für die Verwendung von sicheren Passwörtern deaktiviert. Wenn die Funktion aktiviert wird, müssen Benutzer bei einer Änderung ihres jeweiligen Passworts ein sicheres Passwort angeben. Die alten "nicht sicheren" Passwörter bleiben bis zu einer solchen Passwortänderung gültig.

So richten Sie Beschränkungen für Passwörter ein

1 Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.

2 Wählen Sie in der Serverliste eine Serverkonfiguration aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.

3 Wählen Sie im Hauptmenü **Tools** ▸ **Konten** ▸ **Systemrichtlinie**.

4 Wählen Sie im Register **Passwörter** eine Option für die Gültigkeitsdauer für Passwörter:

- **Passwörter sind unbegrenzt gültig**
- **Passwörter werden ungültig nach ___ Tagen**. Bei dieser Option müssen Sie die Anzahl von Tagen eingeben, für die ein Passwort gültig ist. Die Tage werden ab dem Zeitpunkt gezählt, zu dem das Passwort erstellt wurde.

5 Aktivieren Sie das Auswahlfeld **Sichere Passwörter erforderlich**, wenn Passwörter die folgenden Kriterien erfüllen müssen:

- Neue Passwörter müssen sich von alten unterscheiden.
- Neue Passwörter müssen sich vom Benutzernamen unterscheiden.
- Neue Passwörter müssen Zeichen in Groß- und Kleinschreibung enthalten. Dabei muss jeweils mindestens ein Buchstabe des Alphabets in Groß- bzw. Kleinschreibung verwendet werden. (Maßgeblich hierfür ist das Basisalphabet mit 26 Buchstaben.)
- Neue Passwörter müssen mindestens ein nicht-alphabetisches Zeichen enthalten.

Wenn Sie dieses Auswahlfeld aktivieren, wird der Wert im Textfeld "Mindestlänge des Passworts" auf 3 gesetzt. Sie können diesen Wert erhöhen, wenn Sie möchten.

6 Geben Sie optional eine Zahl für die Mindestlänge des Passworts ein. Der Vorgabewert 0 ermöglicht die Eingabe leerer Passwörter. Die maximale Passwortlänge beträgt 32 Zeichen.

7 Klicken Sie auf **OK**.

Verwandte Verfahrensweisen

Benutzerpasswörter ändern
Passwortänderung erzwingen
Serveradministrations-Tool öffnen

Zugriffsrechte und Gruppenberechtigungen verwalten

Dieser Abschnitt beschreibt Vorgehensweisen zum Verwalten von Zugriffsrechten und Gruppenberechtigungen.

In diesem Abschnitt

Berechtigungen konfigurieren

Als Administrator können Sie Gruppenberechtigungen außer Kraft setzen, indem Sie die Option für die Serverkonfiguration im Dialogfeld **Systemrichtlinie** festlegen. Verwenden Sie diese Optionen mit Vorsicht, da hierdurch die Vorgehensweise des Servers beim Prüfen der Zugriffsrechte aller Benutzer (einschließlich der Administratoren) auf alle Objekte des Repositorys geändert wird. Wenn Berechtigungen nicht berücksichtigt werden, wird ausschließlich durch Zugriffsrechte festgelegt, wer Operationen an Objekten im Repository durchführen darf und wer nicht.

Hinweis: Sie können diese Option nur bei laufenden Serverkonfigurationen ändern.

So verwenden oder ignorieren Sie Gruppenberechtigungen

1. Öffnen Sie das Serveradministrations-Tool und wählen Sie die Serverkonfiguration aus, die Sie ändern möchten.

   Hinweis: Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.

2. Klicken Sie auf die Verknüpfung **Systemrichtlinie** im Verknüpfungsfenster oder wählen Sie **Tools** ▸ **Konten** ▸ **Systemrichtlinie** im Hauptmenü.

   Das Dialogfeld **Systemrichtlinie** wird geöffnet.
3. Wählen Sie das Register **Zugriffsrechte**.
4. Aktivieren oder deaktivieren Sie **Gruppenberechtigungen ignorieren**. Wenn Sie das Auswahlfeld deaktiviert haben, überprüft die Serverkonfiguration, ob Berechtigungen vorhanden sind.
5. Klicken Sie auf **OK** , damit die Änderungen wirksam werden.

Verwandte Konzepte

Zugriffsrechte verweigern
Zugriffsrechte gewähren

Verwandte Verfahrensweisen

Zugriffsrechte und Gruppenberechtigungen verwalten

Verwandte Referenz

Zugriffsrechte und Berechtigungen

Gruppenberechtigungen einrichten

Durch die einer Gruppe zugewiesenen Berechtigungen erhalten Mitglieder der Gruppe möglicherweise das Recht, auf Objekte zuzugreifen und Operationen auszuführen, für die sie normalerweise keine Rechte haben. Mit anderen Worten: Berechtigungen haben Vorrang vor Einstellungen für Zugriffsrechte.

Die Serverkonfiguration wird mit einigen Standardgruppen ("All Users", "Administrators", "System Managers" und "Security Administrators") ausgeliefert, die im Dialogfeld **Benutzer-Manager** angezeigt werden. Der Standardbenutzer mit dem Namen *Administrator* ist Mitglied der Gruppen "Administrators" und "Security Administrators". Standardmäßig verfügt die Administratorengruppe über alle Gruppenberechtigungen. Alle anderen Gruppen verfügen standardmäßig über keine dieser Berechtigungen. Alle Mitglieder einer Gruppe haben für jedes von der Serverkonfiguration verwaltete Projekt dieselben Berechtigungen. Diese Berechtigungen gelten auf allen Ebenen — für Projekte, Ansichten, Ordner und Elemente in Ordnern. Wenn Benutzer mehreren Gruppen angehören, verfügen sie über die maximale Anzahl an Berechtigungen, unabhängig davon, welche Gruppe diese Berechtigungen gewährt.

Hinweis: Berechtigungen können im Dialogfeld **Benutzer-Manager** nur bei aktiviertem Server geändert werden.

So legen Sie Berechtigungen fest

1. Öffnen Sie das Serveradministrations-Tool und wählen Sie die Serverkonfiguration aus, die Sie ändern möchten.

   Hinweis: Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.

2. Klicken Sie im Verknüpfungsfenster auf die Verknüpfung **Benutzer-Manager** oder wählen Sie im Hauptmenü **Tools ▸ Konten ▸ Benutzer-Manager**. Das Dialogfeld **Benutzer-Manager** wird geöffnet.
3. Fügen Sie im Dialogfeld **Benutzer-Manager** eine Gruppe hinzu oder wählen Sie eine Gruppe aus.
4. Fügen Sie der Gruppe bei Bedarf Benutzer hinzu.
5. Klicken Sie mit der rechten Maustaste in der **Gruppen**-Baumstruktur auf den Gruppennamen und wählen Sie im Kontextmenü die Option **Eigenschaften**. Das Dialogfeld **Gruppeneigenschaften** wird angezeigt.
6. Wählen Sie das Register **Berechtigungen**.
7. Aktivieren oder deaktivieren Sie die entsprechenden Auswahlfelder, um der Gruppe die Zugriffsrechte zuzuweisen oder zu entziehen.
8. Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

Verwandte Konzepte

Zugriffsrechte und Gruppenberechtigungen
Zugriffsrechte gewähren

Verwandte Verfahrensweisen

Zugriffsrechte und Gruppenberechtigungen verwalten
Berechtigungen konfigurieren
Benutzer einrichten
Gruppen einrichten

Verwandte Referenz

Zugriffsrechte und Berechtigungen
Gruppenberechtigungen

Zugriffsrechte auf Serverebene festlegen

Durch die Zugriffsrechte auf Serverebene werden Benutzer und Gruppen autorisiert, Operationen in einer bestimmten Serverkonfiguration auszuführen. Eine der Optionen legt fest, wer Projekte erstellen darf, wenn die Serverkonfiguration ausgeführt wird, und wer nicht.

Hinweis: Zugriffsrechte auf Serverebene können nur bei aktiviertem Server zugewiesen werden.

So legen Sie Zugriffsrechte auf Serverebene fest

1. Wählen Sie die zu ändernde Serverkonfiguration im Serveradministrations-Tool aus. Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.
2. Klicken Sie im Verknüpfungsfenster auf die Verknüpfung **Zugriffsrechte** oder wählen Sie **Tools** ▸ **Konten** ▸ **Zugriffsrechte** im Hauptmenü. Das Dialogfeld **Zugriffsrechte** wird geöffnet.
3. Klicken Sie auf **Neu**. Das Dialogfeld **Benutzer oder Gruppe hinzufügen** wird angezeigt.
4. Wählen Sie den Benutzer oder die Gruppe aus, dem bzw. der die Zugriffsrechte zugewiesen werden sollen.
5. Aktivieren Sie die Option **Gewähren** und klicken Sie auf **OK**, um zum Dialogfeld **Zugriffsrechte** zurückzukehren.

   Warnung: Aktivieren Sie niemals die Option **Verweigern**, es sei denn, es handelt sich um eine Ausnahme.

6. Wählen Sie im Dialogfeld **Zugriffsrechte** einen Benutzer oder eine Gruppe aus der Liste **Benutzer und Gruppen** aus. Dadurch werden die verschiedenen Auswahlfelder im Dialogfeld**Zugriffsrechte** aktiviert. Aktivieren und/oder deaktivieren Sie die gewünschten Auswahlfelder. Wenn das Fenster **Zugriffsrechte** nicht vollständig angezeigt wird, ändern Sie die Größe des Serveradministrations-Tool-Fensters.

   Klicken Sie je nach Bedarf auf **Alles auswählen** und **Alles löschen**, um schnell alle Auswahlfelder im Dialogfeld **Zugriffsrechte** zu aktivieren bzw. zu deaktivieren.

   Warnung: Durch Klicken auf **Löschen** wird der ausgewählte Benutzer bzw. die ausgewählte Gruppe aus der Liste **Benutzer und Gruppen** entfernt. Außerdem verliert der Benutzer oder die Gruppe zuvor gewährte Zugriffsrechte für den Server.

7. Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

Verwandte Konzepte

Zugriffsrechte verweigern
Zugriffsrechte gewähren

Verwandte Verfahrensweisen

Zugriffsrechte und Gruppenberechtigungen verwalten

Verwandte Referenz

Serverzugriffsrechte
Zugriffsrechte und Berechtigungen

Zugriffsrechte konfigurieren

Dieses Thema enthält folgende Informationen:

- Zugriffsrechte festlegen (allgemeine Informationen)
- Ausnahmen für Zugriffsrechte erstellen (Datensätze zu verweigerten Rechten)
- Zugriffsrechte für Heraufstufungsstatuswerte auf Projekt- oder Ansichtsebene konfigurieren
- Zugriffsrechte für einzelne Heraufstufungsstatuswerte festlegen
- Zugriffsrechte für Komponenten festlegen
- Zugriffsrechte für einzelne Filter festlegen
- Zugriffsrechte für einzelne Abfragen festlegen

Hinweis: Sie können Zugriffsrechte nur bei laufenden Serverkonfigurationen ändern. Gemeinsam genutzte Ordner oder Elemente verwenden die ursprünglich für sie auf Ordner- oder Elementebene eingerichteten Zugriffsrechte, bis sie an ihrer neuen Position verzweigen. Durch die Verzweigung wird ein neues Objekt erstellt, das zunächst nicht über Zugriffsrechte auf Ordner- oder Elementebene verfügt.

So legen Sie Zugriffsrechte fest (allgemeine Informationen)

1. Wählen Sie im StarTeam-Client das Objekt oder Element aus, für das Rechte festgelegt werden sollen:
   - Damit Sie projektweite Zugriffsrechte einrichten können, muss der Zugriff auf das Projekt über jede Ansicht möglich sein.
   - Damit Sie Zugriffsrechte für eine Ansicht festlegen können, muss diese Ansicht geöffnet sein.
   - Damit Sie Zugriffsrechte für einen Ordner definieren können, müssen Sie den gewünschten Ordner in der Ordnerhierarchie im linken Teilfenster auswählen.
   - Damit Sie Komponentenzugriffsrechte für öffentliche Filter oder Abfragen erstellen können (z. B. für die Änderungsanforderungskomponente), muss im oberen Fenster das Register "Komponente" ausgewählt sein.
   - Damit Sie Zugriffsrechte für einzelne Dateien, Änderungsanforderungen, Anforderungen, Themen oder Tasks festlegen können, müssen Sie das gewünschte Element im oberen Teilfenster auswählen.

2. Wählen Sie im entsprechenden Menü oder Kontextmenü die Option **Zugriffsrechte** wie folgt aus:
   - Zum Festlegen von Zugriffsrechten auf Projektebene wählen Sie die Option **Projekt** ▶ **Zugriffsrechte** im Hauptmenü.
   - Zum Festlegen von Zugriffsrechten auf Ansichtsebene wählen Sie die Option **Ansicht** ▶ **Zugriffsrechte** im Hauptmenü.
   - Zum Festlegen von Zugriffsrechten auf Ordnerebene klicken Sie im Register **Ordner** mit der rechten Maustaste auf den Ordner und wählen Sie**Erweitert** ▶ **Zugriffsrechte** im Kontextmenü.
   - Zum Festlegen von Zugriffsrechten auf Komponentenebene für öffentliche Filter und Abfragen wählen Sie den Komponententyp (z. B. das Menü **Änderungsanforderung**) und anschließend **<Komponententyp>** ▶ **Erweitert** ▶ **Komponentenzugriffsrechte** im Hauptmenü.
   - Zum Festlegen von Zugriffsrechten auf Elementebene wählen Sie im oberen Fenster das Element und anschließend **<Komponententyp>** ▶ **Erweitert** ▶ **Elementzugriffsrechte** im Hauptmenü.

3. Klicken Sie im Dialogfeld **Zugriffsrechte** auf **Hinzufügen**, um einen Benutzer oder eine Gruppe auszuwählen.

Das Dialogfeld **Zugriffsrechte zuweisen für** wird geöffnet.

4 Wählen Sie einen Benutzer oder eine Gruppe aus. Benutzer werden nach ihren Benutzernamen aufgelistet und Gruppen nach ihren Pfaden (mit Ausnahme der Gruppe *All Users*).

5 Wählen Sie **Gewähren** und klicken Sie auf **OK**, um zum Dialogfeld **Zugriffsrechte** zurückzukehren.

> **Warnung:** Wählen Sie niemals den Optionsschalter **Verweigern**, es sei denn, es handelt sich um eine Ausnahme. Verweigerte Rechte müssen vor gewährten Rechten definiert werden.

6 Aktivieren und/oder deaktivieren Sie im Dialogfeld **Zugriffsrechte** die entsprechenden Auswahlfelder. Durch das Aktivieren bzw. Deaktivieren einer Kategorie, z. B. **Allgemeine Rechte für Objekt**, für ein Projekt werden alle Auswahlfelder der Zugriffsrechte dieser Kategorie aktiviert bzw. deaktiviert.

Das Auswahlfeld für die Kategorie weist nur zwei Zustände auf. Ein leeres Auswahlfeld bedeutet, dass die Auswahlfelder für die Zugriffsrechte der Kategorie entweder alle deaktiviert sind oder unterschiedliche Zustände aufweisen: Einige sind aktiviert und andere deaktiviert.

> **Warnung:** Wenn Sie auf **Löschen** klicken, wird der ausgewählte Benutzer oder die Gruppe aus der Liste "Benutzer und Gruppen" im Dialogfeld **Zugriffsrechte** gelöscht. Außerdem verliert der ausgewählte Benutzer oder die Gruppe zuvor festgelegte Zugriffsrechte für den Server.

7 Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

Angenommen, Sie haben eine Gruppe mit dem Namen "Tester", die über vollständigen Zugriff auf die Dateien der Ansicht "QA" verfügt. Diese Ansicht enthält Ordner mit vielen Testdateien. Ein neu eingestelltes Mitglied der Gruppe "Tester" mit dem Namen "Neuer Tester" wurde noch nicht in der Aktualisierung der Tests usw. geschult. Obwohl "Neuer Tester" ein Mitglied der Gruppe "Tester" ist, möchten Sie, dass dieser Benutzer in den folgenden Wochen gewisse Dateioperationen noch nicht ausführt. Sie könnten "Neuer Tester" für diese Zeit aus der Gruppe "Tester" entfernen, aber in der Anwendung haben Sie außerdem die Möglichkeit, "Neuer Tester" alle Rechte der Gruppe "Tester" mit einigen Ausnahmen zuzuweisen. In einem Datensatz zu verweigerten Rechten können Sie diese Ausnahmen aufführen.

So erstellen Sie einen Datensatz zu verweigerten Rechten, um Ausnahmen für Zugriffsrechte festzulegen

1 Klicken Sie im Dialogfeld **Zugriffsrechte** auf **Hinzufügen**.

Das Dialogfeld **Zugriffsrechte zuweisen für** wird geöffnet.

2 Wählen Sie den Benutzer der Gruppe aus, für den die Ausnahme gelten soll.

3 Wählen Sie **Verweigern** und klicken Sie auf **OK**, um zum Dialogfeld **Zugriffsrechte** zurückzukehren.

> **Warnung:** Wählen Sie niemals **Verweigern**, um eine Ausnahme für eine Gruppe zu erstellen, ohne der Gruppe zuvor Zugriffsrechte für den betreffenden Knoten zu gewähren. In diesem Beispiel muss die Gruppe "Tester" über Zugriff auf den Knoten verfügen.

4 Aktivieren und/oder deaktivieren Sie im Dialogfeld **Zugriffsrechte** die entsprechenden Auswahlfelder.

5 Klicken Sie auf **Nach oben**, um den Datensatz zu verweigerten Rechten an den Anfang der Liste **Benutzer und Gruppen** im Dialogfeld **Zugriffsrechte** zu verschieben.

> **Tipp:** Alle verweigerten Rechte müssen vor den gewährten Rechten in der Liste **Benutzer und Gruppen** aufgelistet sein. Anderenfalls können diese Ausnahmen nicht berücksichtigt werden. Wenn die Anwendung beispielsweise die gewährten Rechte für die Tester vor den

verweigerten Rechten für "Neuer Tester" findet, werden die Zugriffsrechte angewendet, die dem Benutzer als Mitglied der Gruppe "Tester" zur Verfügung stehen.

6 Klicken Sie auf **OK** , um die Änderungen zu übernehmen und das Dialogfeld zu schließen.

Hinweis: Aufgrund der Berechtigungen der Gruppe "Tester" ist "Neuer Tester" möglicherweise dennoch in der Lage, die verweigerten Operationen auszuführen.

Außerdem wird, wenn für einen Knoten ausschließlich Zugriffsrechte verweigert werden, allen Benutzern, denen die Zugriffsrechte für diesen Knoten nicht ausdrücklich gewährt wurden, der Zugriff auf den Objekttyp auf dieser Ebene verweigert. Wenn die Anwendung einen Knoten für den entsprechenden Objekttyp findet, der auch nur über einen Datensatz verfügt, werden höhere Ebenen nicht mehr auf Zugriffsrechte geprüft.

Das Festlegen von Zugriffsrechten für Heraufstufungsstatuswerte verläuft ähnlich wie das Festlegen anderer Zugriffsrechte. Die Zugriffsrechte können auf Projekt- oder Ansichtsebene sowie für einzelne Heraufstufungsstatuswerte festgelegt werden.

So legen Sie Zugriffsrechte für Heraufstufungsstatuswerte auf Projekt- oder Ansichtsebene fest

1. Wählen Sie im Hauptmenü **Projekt** ▸ **Zugriffsrechte** oder **Ansicht** ▸ **Zugriffsrechte**. Das Dialogfeld **Zugriffsrechte** wird geöffnet.
2. Wählen Sie den Knoten **Ansicht**.
3. Klicken Sie auf **Hinzufügen**, um einen Benutzer oder eine Gruppe auszuwählen. Das Dialogfeld **Zugriffsrechte zuweisen für** wird geöffnet.
4. Wählen Sie einen Benutzer oder eine Gruppe aus. Benutzer werden nach ihren Benutzernamen aufgelistet und Gruppen nach ihren Pfaden (mit Ausnahme der Gruppe "All Users").
5. Wählen Sie **Gewähren** und klicken Sie auf **OK**, um zum Dialogfeld **Zugriffsrechte** zurückzukehren.
6. Aktivieren und/oder deaktivieren Sie im Dialogfeld **Zugriffsrechte** die entsprechenden Auswahlfelder.
7. Klicken Sie auf **OK** , damit die Änderungen wirksam werden.

So legen Sie Zugriffsrechte für einzelne Heraufstufungsstatuswerte fest

1. Wählen Sie im Hauptmenü **Ansicht** ▸ **Heraufstufung**. Das Dialogfeld **Heraufstufung** wird geöffnet.
2. Wählen Sie im Listenfeld einen Heraufstufungsstatus aus.

Hinweis: Sie können den Heraufstufungsstatus auch im Dialogfeld **Heraufstufung** erstellen. Sie müssen jedoch auf **Übernehmen** klicken, bevor Sie Zugriffsrechte festlegen können. Nach dem Klicken auf **Übernehmen** (oder nach Schließen und erneutem Öffnen des Dialogfelds) kann der Schalter **Zugriffsrechte** ausgewählt werden.

3. Klicken Sie auf **Zugriffsrechte**. Das Dialogfeld **Heraufstufungsstatus - Zugriffsrechte** wird geöffnet.
4. Klicken Sie auf **Hinzufügen**, um einen Benutzer oder eine Gruppe auszuwählen. Das Dialogfeld **Zugriffsrechte zuweisen für** wird geöffnet.
5. Wählen Sie einen Benutzer oder eine Gruppe aus. Benutzer werden nach ihren Benutzernamen aufgelistet und Gruppen nach ihren Pfaden (mit Ausnahme der Gruppe "All Users"). Klicken Sie auf **Gewähren**.
6. Klicken Sie auf **OK**, um zum Dialogfeld **Heraufstufungsstatus - Zugriffsrechte**zurückzukehren.
7. Aktivieren und/oder deaktivieren Sie die entsprechenden Auswahlfelder und klicken Sie auf **OK**, damit die Änderungen wirksam werden und das Dialogfeld **Heraufstufungsstatus - Zugriffsrechte** geschlossen wird.

8 Klicken Sie auf **OK**, um das Dialogfeld **Heraufstufung** zu beenden.

Wenn Sie auf Serverebene über das Zugriffsrecht **Zugriffsrechte für Komponenten verwalten** verfügen, können Sie auf Komponentenebene Zugriffsrechte für alle geöffneten Komponenten festlegen.

So legen Sie Zugriffsrechte auf Komponentenebene fest

1. Öffnen Sie eine Projektansicht, für die Sie die notwendigen Zugriffsrechte besitzen.
2. Wählen Sie das Register mit der gewünschten Komponente (Datei, Änderungsanforderung usw.) aus.
3. Wählen Sie im Hauptmenü <Komponententyp> ▸ Erweitert ▸ Komponentenzugriffsrechte. Das Dialogfeld **<Komponententyp> Komponentenzugriffsrechte** wird geöffnet.
4. Markieren Sie den entsprechenden Knoten:
   - Wählen Sie den Knoten **Komponente**, um zu steuern, wer öffentliche Filter und Abfragen für die Komponente erstellen darf.
   - Wählen Sie den Knoten **Filter**, um zu steuern, wer öffentliche Filter auf die Komponente anwenden darf.
   - Wählen Sie den Knoten **Abfrage**, um zu steuern, wer öffentliche Abfragen auf die Komponente anwenden darf.
5. Fügen Sie einen Benutzer oder eine Gruppe hinzu:
   1. Klicken Sie auf **Hinzufügen**, um das Dialogfeld **Zugriffsrechte zuweisen für** anzuzeigen.
   2. Wählen Sie einen Benutzer oder eine Gruppe aus und klicken Sie anschließend auf **Gewähren**.
   3. Klicken Sie auf **OK**, um zum Dialogfeld **<Komponententyp> Komponentenzugriffsrechte** zurückzukehren.

   Warnung: Wählen Sie niemals die Option **Verweigern** im Dialogfeld **Zugriffsrechte zuweisen für**, es sei denn, es handelt sich um eine Ausnahme.

6. Aktivieren und/oder deaktivieren Sie im Dialogfeld **<Komponententyp> Komponentenzugriffsrechte** die entsprechenden Auswahlfelder.

   Hinweis: Durch Klicken auf **Löschen** wird der ausgewählte Benutzer bzw. die ausgewählte Gruppe aus der Liste **Benutzer und Gruppen** entfernt. Der ausgewählte Benutzer oder die Gruppe verliert zuvor gewährte Zugriffsrechte für die Filter und Abfragen dieser Komponente.

7. Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

So legen Sie Zugriffsrechte für einen Filter fest

1. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie im oberen Fenster mit der rechten Maustaste auf einen Spaltentitel und wählen Sie Filter im Kontextmenü.
   - Wählen Sie Filter ▸ Filter im Haupt- oder Kontextmenü der entsprechenden Komponente (Datei, Änderungsanforderung, Anforderung, usw.).

   Das Dialogfeld **Filter** wird geöffnet.
2. Wählen Sie den Filter aus und klicken Sie auf **Zugriffsrechte**. Das Dialogfeld **Filter <Filtername> - Zugriffsrechte** wird geöffnet.

3 Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Zugriffsrechte zuweisen für** wird geöffnet.

4 Wählen Sie einen Benutzer oder eine Gruppe aus. Benutzer werden nach ihren Benutzernamen aufgelistet und Gruppen nach ihren Pfaden (mit Ausnahme der Gruppe "All Users").

5 Wählen Sie **Gewähren** und klicken Sie auf **OK**, um zum Dialogfeld **Filter <Filtername> - Zugriffsrechte** zurückzukehren.

> **Warnung:** Wählen Sie niemals die Option **Verweigern** im Dialogfeld **Zugriffsrechte zuweisen für**, es sei denn, es handelt sich um eine Ausnahme.

6 Aktivieren und/oder deaktivieren Sie im Dialogfeld **Filter <Filtername> - Zugriffsrechte** die entsprechenden Auswahlfelder.

> **Hinweis:** Durch Klicken auf **Löschen** wird der ausgewählte Benutzer bzw. die ausgewählte Gruppe aus der Liste **Benutzer und Gruppen** entfernt. Außerdem verliert der ausgewählte Benutzer oder die Gruppe zuvor festgelegte Zugriffsrechte für den Filter.

7 Klicken Sie auf **OK**, um die Änderungen zu übernehmen und das Dialogfeld **Filter <Filtername> - Zugriffsrechte** zu schließen.

8 Klicken Sie auf **OK**, um das Dialogfeld **Filter** zu schließen.

So legen Sie Zugriffsrechte für eine Abfrage fest

1 Führen Sie einen der folgenden Schritte aus:

- Klicken Sie im oberen Fenster mit der rechten Maustaste auf einen Spaltentitel und wählen Sie **Abfragen** im Kontextmenü.
- Wählen Sie **Filter** ▸ **Abfragen** im Haupt- oder Kontextmenü der entsprechenden Komponente (Datei, Änderungsanforderung, Anforderung, usw.).

Das Dialogfeld **Abfragen** wird geöffnet.

2 Wählen Sie die Abfrage aus und klicken Sie auf **Zugriffsrechte**. Das Dialogfeld **Abfrage <Name der Abfrage> - Zugriffsrechte** wird geöffnet.

3 Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Zugriffsrechte zuweisen für** wird geöffnet.

4 Wählen Sie einen Benutzer oder eine Gruppe aus. Benutzer werden nach ihren Benutzernamen aufgelistet und Gruppen nach ihren Pfaden (mit Ausnahme der Gruppe "All Users").

5 Wählen Sie **Gewähren** und klicken Sie auf **OK**, um zum Dialogfeld **Abfrage <Name der Abfrage> - Zugriffsrechte** zurückzukehren.

> **Warnung:** Wählen Sie niemals die Option **Verweigern** im Dialogfeld **Zugriffsrechte zuweisen für**, es sei denn, es handelt sich um eine Ausnahme.

6 Aktivieren und/oder deaktivieren Sie im Dialogfeld **Abfrage <Name der Abfrage> - Zugriffsrechte** die entsprechenden Auswahlfelder.

> **Hinweis:** Durch Klicken auf **Löschen** wird der ausgewählte Benutzer bzw. die ausgewählte Gruppe aus der Liste **Benutzer und Gruppen** entfernt. Außerdem verliert der ausgewählte Benutzer oder die Gruppe zuvor festgelegte Zugriffsrechte für die Abfrage.

7 Klicken Sie auf **OK**, um die Änderungen zu übernehmen und das Dialogfeld **Abfrage <Name der Abfrage> - Zugriffsrechte** zu schließen.

8 Klicken Sie auf **OK**, um das Dialogfeld **Abfragen** zu schließen.

Verwandte Konzepte

Zugriffsrechte gewähren
Zugriffsrechte verweigern

Verwandte Verfahrensweisen

Zugriffsrechte und Gruppenberechtigungen verwalten

Verwandte Referenz

Zugriffsrechte und Berechtigungen

Protokoll- und Initialisierungsdateien verwalten

Dieser Abschnitt beschreibt Vorgehensweisen zum Verwalten von Protokoll- und Initialisierungsdateien.

In diesem Abschnitt

'StarTeam.Log' anzeigen und anpassen

In der StarTeam.Log-Datei werden alle Operationen protokolliert, die auf Ihrer Client-Workstation während einer Sitzung durchgeführt wurden. Die Datei dokumentiert Fehler und fehlgeschlagene Operationen zwischen dem Server und Ihrer Workstation während Serverkonfigurationssitzungen, sodass die Ursachen der Fehler leichter erkannt werden können.

Da die Anwendung bei jedem Start des Clients eine neue StarTeam.Log-Datei erstellt, wächst die Größe des Ordners für die StarTeam-Protokolldatei möglicherweise sehr schnell an. Um die Anzahl der Protokolldateien in dem Ordner zu steuern, sollten Sie regelmäßig alte Protokolldateien aus dem Ausgabeordner löschen oder die StarTeam.Log-Option deaktivieren. Um diese Option zu deaktivieren, heben Sie die Markierungen der Auswahlfelder für Protokollfehler und Protokolloperationen im Register "Arbeitsbereich" des Dialogfelds "Persönliche Optionen" auf. Wählen Sie zum Anzeigen der StarTeam.Log-Datei in der Menüleiste **Tools** ▸ **StarTeam-Protokolldatei**. Sie können außerdem Daten aus einer StarTeam.Log-Datei in eine Anwendung importieren, die kommagetrennte Felder unterstützt, und in dieser anzeigen. Wenn Sie die Datei beispielsweise mit einer .csv-Erweiterung speichern, können Sie sie in Microsoft Excel öffnen.

Im Register "Arbeitsbereich" können Sie im Dialogfeld "Persönliche Optionen" den Speicherort der Datei "StarTeam.Log" und den Typ der im Protokoll aufzuzeichnenden Daten festlegen.

So passen Sie die StarTeam.Log-Datei an

1. Wählen Sie im Client **Tools** ▸ **Persönliche Optionen**. Das Dialogfeld **Persönliche Optionen** wird angezeigt.
2. Geben Sie im Register **Arbeitsbereich** im Textfeld **Ausgabepfad für Protokoll** einen Speicherort für die StarTeam.Log-Datei ein oder suchen Sie nach dem Pfad. Vorgegeben ist der Speicherort, an der die Anwendung installiert ist, beispielsweise `C:\Dokumente und Einstellungen\<Benutzername>\Anwendungsdaten\Borland\StarTeam`. Die aktuelle Protokolldatei heißt immer "StarTeam.log". Protokolldateien vorhergehender Sitzungen enthalten immer das Datum und die Uhrzeit des Zeitpunkts, zu dem die Datei zuletzt geändert wurde.

   Hinweis: Die Datei "StarTeam.log" enthält Daten zu Operationen, die je nach der von Ihnen geöffneten Projektansicht von Ihrer Workstation an einen oder mehrere Server gesendet wurden. Dazu gehört der Projektname, damit Sie bei Bedarf Daten für einen bestimmten Server einzeln anzeigen können.

3. Wählen Sie die Datentypen aus, die in der StarTeam.Log-Protokolldatei aufgezeichnet werden sollen.
   - Fehler protokollieren - Diese Option ist standardmäßig aktiviert. Zeichnet Fehler auf, die bei der Ausführung eines Clients auftreten. Das Fehlerprotokoll zeichnet den Start der Serverkonfiguration mit Datum und Uhrzeit auf sowie alle Fehler oder fehlgeschlagenen Operationen zwischen dem Server und dem Client. Die Anwendung markiert jede fehlgeschlagene Operation durch eine interne ID und bietet eine Erklärung an. Beispielsweise könnte Ihnen Folgendes angezeigt werden:`...Operation 40956 fehlgeschlagen: TCP/IP Socket-Fehler 10054:...`
   - StarTeamMPX-Ereignisse protokollieren - Wenn Sie diese Option auswählen, werden Informationen über StarTeamMPX-Ereignisse für diesen Client aufgezeichnet. Das Protokoll gibt die Uhrzeit und das Datum von StarTeamMPX-Ereignissen (z. B. eine automatische Aktualisierung oder eine Aktualisierung des Dateistatus) an. StarTeamMPX-Ereignissen wird im Protokoll der Eintrag "Statistics for Events" vorangestellt, und sie werden durch interne IDs und kurze Erklärungen gekennzeichnet. Das folgende Beispiel beschreibt eine Statusänderung für eine Datei:`...Statistics for Events /1b21dd1-e208-51ea-01b2-1dd1e20851ea/Object/File/ Modify` Sie können StarTeamMPX-Ereignisse nur protokollieren, wenn das Auswahlfeld "StarTeamMPX aktivieren" im Register "StarTeamMPX" markiert ist. Bei StarTeamMPX-Operationen werden Änderungen, die Sie im Register "Arbeitsbereich" vornehmen, nicht auf bereits geöffnete Projekte angewendet. Die Anwendung protokolliert jedoch StarTeamMPX-Ereignisse für alle Projekte, die ab diesem Zeitpunkt geöffnet werden.

- Operationen und Ereignisse protokollieren mit einer Mindestdauer von ___Millisekunden Wählen Sie diese Option aus, um Operationen aufzuzeichnen, die länger als eine festgelegte Anzahl von Millisekunden gedauert haben. (Eine Operation ist ein Befehl, der durch Benutzer-Aktionen initiiert wird. Operationen können sowohl auf dem Server als auch auf dem Client ausgeführt werden.) Die Zeitbegrenzung in Millisekunden verhindert, dass das Protokoll mit nebensächlichen Operationen gefüllt wird. Der Standardwert ist 10 Millisekunden. Mit dieser Option werden das Datum, die Uhrzeit und die Benutzerschnittstellen-Operationsnummer für alle Befehle aufgezeichnet, die auf Ihrer Workstation ausgeführt werden. Sie können entweder zusammengefasste oder detaillierte Informationen aufzeichnen.

- Wenn Sie "Zusammenfassung" auswählen, werden die Gesamtdauer der Operation, die Client-Ausführungszeit und die Server-Ausführungszeit protokolliert. Die Anwendung kennzeichnet jede Operation mit einer internen ID, z. B. "Statistics for Operation 40001".
- Wenn Sie "Detail" auswählen, wird eine detaillierte Aufstellung aller Serverbefehle für jede durchgeführte Operation aufgezeichnet. Das Protokoll gibt die Serveradresse, das Projekt und die Komponente (Datei, Änderungsanforderung, Anforderung, Task oder Thema) für jeden Serverbefehl an. Die Anwendung kennzeichnet jeden Serverbefehl mit einer internen ID, z. B. "Public Server Command 10".

4 Klicken Sie auf **OK**, sobald Sie fertig sind.

Verwandte Verfahrensweisen

Initialisierungsdateien suchen
Das Audit-Protokoll aktivieren und bereinigen
Mit dem Serverprotokoll arbeiten
Mit dem Sicherheitsereignisprotokoll arbeiten

Das Audit-Protokoll aktivieren und bereinigen

Wenn Sie die Option "Audit-Generierung aktivieren" auswählen, protokolliert der Server Audit-Ereignisse für StarTeam-Projekte in der Datenbank für die Serverkonfiguration. Im Protokoll wird beispielsweise aufgezeichnet, wann Änderungsanforderungen erstellt und Dateien hinzugefügt werden. Die Einträge des Audit-Protokolls werden im Client angezeigt, wenn Sie im oberen Teilfenster das Register "Audit" auswählen. Diese Operation kann nur bei gestartetem Server ausgeführt werden.

Hinweis: Wenn Sie die Option zum Bereinigen von Protokollen beim Starten der Serverkonfiguration einstellen, müssen Sie Ihre Serverkonfigurationen regelmäßig neu starten, damit Probleme beim Programmstart vermieden werden.

So aktivieren Sie das Audit-Protokoll

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.
2. Wählen Sie die zu ändernde Serverkonfiguration in der Serverliste aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.
3. Klicken Sie auf die Verknüpfung **Server konfigurieren** oder wählen Sie **Tools** > **Administration** > **Server konfigurieren**. Das Dialogfeld **Server konfigurieren** wird geöffnet.
4. Klicken Sie auf das Register **Audits**.
5. Aktivieren Sie das Auswahlfeld **Audit-Generierung aktivieren**.
6. Optional können Sie das Auswahlfeld **Audit-Einträge entfernen, die älter sind als** auswählen, damit Einträge automatisch nach Ablauf eines bestimmten Zeitraums gelöscht werden. (Wenn das Auswahlfeld nicht aktiviert ist, werden die Einträge nie gelöscht.) Geben Sie in das Textfeld "Tage" eine Anzahl von Tagen ein. Der Wert muss zwischen 7 und 1000 Tagen liegen. Um beispielsweise Einträge zu löschen, wenn sie ca. einen Monat alt sind, geben Sie in das Textfeld "Tage" die Zahl 30 ein. Beim Start der Serverkonfiguration werden Einträge gelöscht, die dieses Bereinigungszeitlimit überschreiten.
7. Klicken Sie auf **OK**.

Verwandte Verfahrensweisen

Mit dem Serverprotokoll arbeiten
Mit dem Sicherheitsereignisprotokoll arbeiten
'StarTeam.Log' anzeigen und anpassen
Initialisierungsdateien suchen
Serveradministrations-Tool öffnen

Mit dem Serverprotokoll arbeiten

Sie können den Inhalt der Serverprotokolldatei jederzeit anzeigen, sogar während die Serverkonfiguration ausgeführt wird. Nur die letzten 64 KB der Protokolldateidaten werden angezeigt. Die gesamte Datei kann im Windows-Editor, in WordPad oder in einem anderen Texteditor angezeigt werden.

So ermitteln Sie den Speicherort einer Serverprotokolldatei über das Serveradministrations-Tool

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.
2. Wählen Sie die entsprechende Serverkonfiguration in der Serverliste aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.
3. Klicken Sie auf die **Verknüpfung "Server konfigurieren"** oder wählen Sie **Tools** ▶ **Administration** ▶ **Server konfigurieren**. In beiden Fällen wird das Dialogfeld **Server konfigurieren** angezeigt.
4. Suchen Sie im oberen Bereich des Registers **Allgemein** nach dem Speicherort der Protokolldatei.

So prüfen Sie den Inhalt einer Serverprotokolldatei

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.
2. Wählen Sie die entsprechende Serverkonfiguration in der Serverliste aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.
3. Klicken Sie auf die Verknüpfung **Serverprotokoll** oder wählen Sie **Tools Administration Serverprotokoll**. Der Inhalt des Serverprotokolls wird angezeigt.

   Das Format setzt sich aus Zeilennummern, Codes, Datums- und Zeitangaben und den Meldungen zusammen. Die Codenummern sind beliebig und werden nicht unbedingt in der Reihenfolge des Schweregrads vergeben. Sie bezeichnen Folgendes:

   ```
   00000001 Meldung
   00000002 Warnung
   00000004 Fehler
   00000008 Unerwarteter Zustand
   ```

4. Aktivieren Sie das Auswahlfeld **Nur Fehler**, wenn nur die Fehler im Protokoll angezeigt werden sollen.
5. Klicken Sie auf **Neu laden**, um die neuesten Einträge anzuzeigen.

Auf Windows-Systemen können Sie Daten aus dem Protokollfenster in die Windows-Zwischenablage kopieren. Aus der Zwischenablage können diese Daten in andere Anwendungen wie Microsoft Word oder den Windows-Editor eingefügt werden.

So kopieren Sie Daten aus dem Serverprotokoll

1. Klicken Sie im Serveradministrations-Tool auf die Leiste **Konten** im unteren linken Fenster und wählen Sie die Verknüpfung **Serverprotokoll**.
2. Wählen Sie die zu kopierenden Daten aus.
3. Drücken Sie STRG + C.
4. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

5 Fügen Sie die Informationen mit STRG + V in einen Texteditor oder ein Textverarbeitungsprogramm ein.

6 Drucken Sie die Daten, indem Sie im Menü **Datei** ▸ **Drucken** wählen.

Alle Benutzer der Standardgruppe "System Managers" erhalten eine E-Mail, wenn ein Fehler im Protokoll aufgezeichnet wird. Diese Gruppe ist anfänglich leer. Informationen zum Hinzufügen von Benutzern zu der Gruppe "System Managers" finden Sie unter dem Link "Benutzer einrichten" am Ende dieses Themas.

Verwandte Verfahrensweisen

Das Audit-Protokoll aktivieren und bereinigen
Mit dem Sicherheitsereignisprotokoll arbeiten
'StarTeam.Log' anzeigen und anpassen
Initialisierungsdateien suchen
Serveradministrations-Tool öffnen
Benutzer einrichten

Mit dem Sicherheitsereignisprotokoll arbeiten

Wenn Sie über Zugriffsrechte für eine Serverkonfiguration verfügen, können Sie das entsprechende Sicherheitsereignisprotokoll jederzeit anzeigen. Das Sicherheitsereignisprotokoll ist keine gewöhnliche .Log-Datei, da die Daten des Protokolls in der Anwendungsdatenbank gespeichert werden. Diese Operation kann nur bei aktiviertem Server ausgeführt werden.

So zeigen Sie das Sicherheitsereignisprotokoll an:

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.
2. Wählen Sie die entsprechende Serverkonfiguration in der Serverliste aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.
3. Wählen Sie **Tools** ▸ **Konten** ▸ **Sicherheitsprotokoll**. Der Inhalt des Sicherheitsprotokolls wird angezeigt. Das Protokoll enthält eine Auflistung aller geschützten Ereignisse (z. B. das An- oder Abmelden), Datums- und Zeitangaben der Ereignisse, die ausführenden Benutzer der Operationen, die Workstations, auf denen die Operationen ausgeführt wurden, die Elemente, für die die Aktionen ausgeführt wurden, und Informationen darüber, ob die Operationen fehlgeschlagen sind.
4. Verwenden Sie das Dropdown-Listenfeld **Sicherheitsereignistyp**, um alle Ereignisse eines bestimmten Typs anzuzeigen.
5. Um das Sicherheitsereignisprotokoll erneut zu laden und die letzten Einträge zu prüfen, klicken Sie im Dialogfeld **Sicherheitsereignisprotokoll** auf **Neu laden**.
6. Um die aus dem Protokoll ausgewählten Daten zu drucken, klicken Sie im Dialogfeld **Sicherheitsereignisprotokoll** auf **Auswahl drucken**.

Abhängig von der Anzahl der Benutzer und dem Umfang der Aktivitäten in einer Serverkonfiguration kann das Sicherheitsereignisprotokoll sehr schnell anwachsen. Der Server kann alte Einträge löschen, um die Größe des Protokolls auf ein vernünftiges Maß zu beschränken. Entscheiden Sie zunächst, wie lange Sicherheitsereignisse gespeichert werden sollen, und legen Sie anschließend in der Serverkonfiguration fest, dass ältere Einträge gelöscht werden. Diese Operation kann nur bei aktiviertem Server ausgeführt werden.

So legen Sie das Intervall für die Bereinigung des Sicherheitsereignisprotokolls fest:

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.
2. Wählen Sie die entsprechende Serverkonfiguration in der Serverliste aus. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.
3. Klicken Sie im Menü auf **Tools** ▸ **Konten** ▸ **Systemrichtlinie**. Das Dialogfeld **Systemrichtlinie** wird angezeigt.
4. Wählen Sie das Register **Sicherheitsereignisse**.
5. Aktivieren Sie das Auswahlfeld **Sicherheitseinträge entfernen, die älter sind als __ Tage**. (Wenn das Auswahlfeld nicht aktiviert ist, werden die Einträge nie gelöscht.)
6. Geben Sie in das Textfeld eine Anzahl von Tagen ein. Der zulässige Bereich liegt zwischen 30 und 1000. Der Vorgabewert ist 180. Beim nächsten Start der Serverkonfiguration werden Einträge gelöscht, die älter als der angegebene Wert sind.
7. Klicken Sie auf **OK**.
8. Starten Sie die Serverkonfiguration neu, damit das Bereinigungsintervall wirksam wird.

Verwandte Verfahrensweisen

Das Audit-Protokoll aktivieren und bereinigen
Mit dem Serverprotokoll arbeiten
'StarTeam.Log' anzeigen und anpassen
Initialisierungsdateien suchen
Serveradministrations-Tool öffnen

Verwandte Referenz

Sicherheitsereignistypen

Informationen sichern

In diesem Abschnitt sind Verfahrensweisen zum Sichern von Informationen beschrieben.

In diesem Abschnitt

Projektdaten sichern

Beim Erstellen von Serverkonfigurationen legt der Server Dateien und Ordner an, in denen Ihre Konfiguration und die Projektdaten gespeichert werden. In der mit der Anwendung gelieferten Beispielkonfiguration *StarDraw* legt der Server beispielsweise den Hive (ein Unterordner im Repository *StarDraw*) mit den Unterordnern *Archives* und *Cache* sowie den Ordner *Attachments* im Repository ab. Das *StarDraw-Repository* enthält zudem den Ordner *Database* mit den SSE-Datenbankinformationen (die .mdf-Datei). In anderen Serverkonfigurationen befinden sich die Datenbankdateien jedoch an einem separaten Speicherort.

Das Repository Ihrer Serverkonfiguration kann Abweichungen aufweisen, die zugrunde liegende Ordnerstruktur ist jedoch auf jeden Fall ähnlich. Sie können den Speicherort der Repository-Ordner ggf. über das Dialogfeld **StarTeam-Serverkonfiguration** oder das Dialogfeld **Hive-Manager** im Serveradministrations-Tool ändern.

So erstellen Sie ein Backup einer Serverkonfiguration

1. Sichern Sie die erforderlichen Repository-Informationen:
   - Den Ordner *HiveIndex*
   - Den Ordner *Archives* des Datenspeichers
   - Den Ordner *Attachments*

2. Erstellen Sie ein Backup der Datenbank:
   - Es ist empfehlenswert, SQL Server-Datenbanken als vollständige Datenbank-Backups zu sichern.
   - Für Oracle-Datenbanken sollten RMAN-Backups erstellt werden.

3. Erstellen Sie eine Sicherungskopie der Datei `starteam-server-configs.xml` .

Hinweis: Stellen Sie sicher, dass Sie Ihre Backups regelmäßig überprüfen. Borland empfiehlt, dass Sie die Backups Ihrer Projektdaten auf einem Testsystem wiederherstellen und testen. So können Sie sicherstellen, dass Ihre Daten korrekt gesichert wurden.

Verwandte Konzepte

Zu sichernde Komponenten
Native-II-Datenspeicher und Hives
StarTeam Backups
Übersicht über die Datenspeicherung
Backups von Oracle-Datenbanken
Backups von SQL Server-Datenbanken
Backups
StarDraw (Beispiel-Serverkonfiguration)

Verwandte Verfahrensweisen

Optionen für die Datenspeicherung konfigurieren
Projektdaten wiederherstellen

Projektdaten wiederherstellen

Stellen Sie sicher, dass Sie Ihre Backups regelmäßig überprüfen. Borland empfiehlt, dass Sie die Backups Ihrer Projektdaten auf einem Testsystem wiederherstellen und testen. So können Sie sicherstellen, dass Ihre Daten korrekt gesichert wurden.

So stellen Sie eine Serverkonfiguration aus einem Backup wieder her

1. Stellen Sie die Datenbank wieder her.
2. Stellen Sie die Repository-Informationen wieder her.
3. Stellen Sie die Datei `starteam-server-configs.xml` wieder her.
4. Starten Sie die Serverkonfiguration.
5. Testen Sie die Serverkonfiguration.

   Sie können die Severkonfiguration testen, indem Sie alle regulären Vorgänge ausführen, z. B. unterschiedliche aktuelle und historische Konfigurationen der wichtigsten Projekte auschecken, den Build-Prozess ausführen usw.

Hinweis: Wenn Sie die Serverkonfiguration auf einen neuen Computer verschieben, müssen Sie auch StarTeam-Server installieren und eine ODBC-Verbindung herstellen.

Verwandte Konzepte

Zu sichernde Komponenten
Native-II-Datenspeicher und Hives
StarTeam Backups
Übersicht über die Datenspeicherung
Backups von Oracle-Datenbanken
Backups von SQL Server-Datenbanken
Backups
StarDraw (Beispiel-Serverkonfiguration)
Übersicht über das Verschieben von Serverkonfigurationen

Verwandte Verfahrensweisen

Optionen für die Datenspeicherung konfigurieren
Projektdaten sichern

Daten aus Auscheckvorgängen verfolgen

Die Themen in diesem Abschnitt beschreiben, wie Sie das Checkout Trace-Dienstprogramm aktivieren und mit diesem Dienstprogramm `*.csv`-Dateien für eine Serverkonfiguration erstellen.

In diesem Abschnitt

.CSV-Dateien zu Auscheckvorgängen generieren
In diesem Thema wird beschrieben, wie Sie das Checkout Trace-Dienstprogramm ausführen und die *.csv-Datei mit Daten zu den Auscheckvorgängen generieren können.

Ablaufverfolgung (Tracing) für Serverkonfigurationen aktivieren
Dieses Thema beschreibt, wie die Ablaufverfolgung zur Verwendung mit dem Checkout Trace-Dienstprogramm für Serverkonfigurationen aktiviert wird.

.CSV-Dateien zu Auscheckvorgängen generieren

Bevor Sie das Dienstprogramm ausführen, müssen Sie die Ablaufverfolgung für die Serverkonfiguration aktivieren. Bei aktivierter Ablaufverfolgung generiert der Server für jede ausgecheckte Datei einen Trace-Datensatz und speichert die Informationen in einer Trace-Datei (`Checkout.cotrc`). Das Dienstprogramm verwendet die Trace-Datei als Input und liefert eine `*.csv`-Datei mit Daten zu den Auscheckvorgängen.

Das Checkout Trace-Dienstprogramm nimmt eine oder mehrere Checkout Trace-Dateien (`*.cotrc`) als Input und liefert eine `*.csv`-Textdatei als Output. Diese Datei enthält Daten zu den Auscheckvorgängen, wobei die einzelnen Werte durch Komma getrennt sind. Der Standardname der `.csv`-Datei ist identisch mit dem Namen der Trace-Datei und hat zusätzlich die Erweiterung `.csv`. Lautet der Name der Trace-Datei beispielsweise `Checkout.cotrc`, dann lautet der Name der `csv`-Ausgabedatei `Checkout.cotrc.csv`.

So führen Sie das Checkout Trace -Dienstprogramm aus

1. Wechseln Sie in der Befehlszeile zum Stammordner des StarTeam-Server-Programms, in dem sich die Datei `CheckoutTraceDump.exe` befindet.
2. Die Option `-go` signalisiert dem Dienstprogramm, dass es mit den Standardoptionen ausgeführt werden soll. Für das Dienstprogramm können Sie viele Parameter setzen. Eine Liste der verfügbaren Befehlszeilenoptionen für dieses Dienstprogramm finden Sie unter dem Link, der am Ende dieses Themas aufgeführt ist.

   Hinweis: Standardmäßig speichert der Server die Trace-Dateien im Trace-Ordner (einem Unterordner des Repository-Ordners `Checkout.cotrc`). Sie können das Dienstprogramm mit der aktuellen Trace-Datei ausführen, sie können aber dazu auch eine Kopie der Trace-Datei verwenden.

Tipp: Wenn Sie das Dienstprogramm nicht vom Server, sondern von einer Workstation aus starten möchten, können Sie die Dateien `CheckoutTraceDump.exe` und `OSSup.dll` an den gewünschten Speicherort kopieren. *Verschieben* Sie bitte die Datei `OSSup.dll` nicht an den neuen Speicherort, da diese Datei auch für die Serverkonfiguration erforderlich ist. Das Dienstprogramm hängt zudem von Microsoft .NET Runtime ab. Diese muss ebenfalls auf der Workstation verfügbar sein.

Verwandte Konzepte

Daten von Auscheckvorgängen mit dem Checkout Trace-Dienstprogramm untersuchen

Verwandte Verfahrensweisen

Ablaufverfolgung (Tracing) für Serverkonfigurationen aktivieren

Ablaufverfolgung (Tracing) für Serverkonfigurationen aktivieren

Wenn Sie die Ablaufverfolgung für eine Serverkonfiguration aktivieren, speichert der Server für jede Datei, die ausgecheckt wird, einen Trace-Datensatz in eine Trace-Datei (`check-out.cotrc`). Sie können diese Trace-Datei anschließend als Input für das Checkout Trace-Dienstprogramm zum Generieren einer `*.csv`-Datei verwenden, die Informationen zu Auscheckvorgängen enthält.

So aktivieren Sie die Ablaufverfolgung für eine Serverkonfiguration

1. Öffnen Sie die Datei `starteam-server-configs.xml`. Sie finden die Datei im Stammordner des StarTeam-Server-Programms.
2. Setzen Sie für jede Serverkonfiguration, für die die Ablaufverfolgung aktiviert werden soll, folgende Optionen auf den Wert `"1"`:

   ```
   <option name="FileAllowCheckoutTrace" value="1"/>
   ```

   ```
   <option name="FileEnableCheckoutTrace" value="1"/>
   ```

   Die erste Option aktiviert den Tracing-Code. Die zweite Option aktiviert bzw. deaktiviert die Ablaufverfolgung. Der Wert `"1"` bedeutet "Wahr" oder ein. Der Wert `"0"` bedeutet "Falsch" oder aus. Um die Ablaufverfolgung zu aktivieren, müssen beide Werte `"1"` sein.
3. Speichern Sie die Änderungen an `starteam-server-configs.xml`.
4. Beenden Sie die Serverkonfiguration und starten Sie sie neu, damit sie die Änderungen an `starteam-server-configs.xml` erkennen kann.

Wenn Sie beide Optionen in `starteam-server-configs.xml` auf `"1"` setzen, erstellt die Serverkonfiguration `Checkout.cotrc`-Dateien im Ordner *Trace* (einem Unterordner des Repository-Ordners `Checkout.cotrc`). Erreicht die Größe der aktuellen Trace-Datei 128 MB, speichert der Server die aktuelle Trace-Datei und erstellt eine neue Trace-Datei. Der Name der älteren Trace-Datei besteht aus dem Namen plus einem Zeitstempel, vergleichbar mit der Namenskonvention für die `server.log`-Dateien von StarTeam. WennSie die Serverkonfiguration beenden, speichert der Server die Trace-Datei mit einem Zeitstempel, der an den Dateinamen angehängt wird. Wenn Sie die Serverkonfiguration neu starten, erstellt der Server eine neue Trace-Datei.

Hinweis: Um die Leistung zu optimieren, aktualisiert StarTeam Trace-Dateien nicht sofort. StarTeam puffert die Informationen für die Trace-Datei im Speicher und schreibt sie zu Zeiten geringer Speicherauslastung in die Trace-Datei.

Verwandte Konzepte

Daten von Auscheckvorgängen mit dem Checkout Trace-Dienstprogramm untersuchen

Verwandte Verfahrensweisen

.CSV-Dateien zu Auscheckvorgängen generieren

Mit Serverkonfigurationen arbeiten

In diesem Abschnitt werden Verfahrensweisen beim Arbeiten mit Serverkonfigurationen beschrieben.

In diesem Abschnitt

Bei der Serverkonfiguration mithilfe des Serveradministrations-Tool anmelden

Wenn Sie Aktualisierungen administrativer Art oder an Konten einer Serverkonfiguration vornehmen müssen, zeigt das Serveradministrations-Tool das Dialogfeld **Anmelden** an.

Dieses Thema enthält folgende Informationen:

- Bei der Serverkonfiguration anmelden.
- Unter anderem Benutzernamen anmelden

So melden Sie sich im Serveradministrations-Tool bei einer Serverkonfiguration an:

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.
2. Wählen Sie im Serverfenster die Serverkonfiguration aus und wählen Sie beliebige administrative Aufgaben oder Konten betreffende Menübefehle, Symbolleistenschalter oder Verknüpfungen aus. Das Dialogfeld **Anmelden** wird angezeigt.
3. Geben Sie den **Benutzernamen** und das **Passwort** ein.

   Tipp: Es gibt für jede Serverkonfiguration einen Standardbenutzernamen und ein -passwort (`Administrator/Administrator`), sofern sie nicht vom Serveradministrator geändert oder gelöscht wurden.

4. (Optional nur für das clientseitig installierte Serveradministrations-Tool) Aktivieren Sie die Option **Als Standard-Anmeldeinformationen für diesen Server speichern**. Ihre Serverkonfigurationsinformationen werden im Toolbar-Dienstprogramm gespeichert.
5. Klicken Sie auf **OK**.

Sobald sich ein Benutzer angemeldet hat, wird der Benutzername in Klammern neben dem Serverkonfigurationsnamen angezeigt. Wenn Sie sich beispielsweise bei der *StarDraw* -Serverkonfiguration mit dem vorgegebenen Benutzernamen *Administrator* anmelden, erhalten Sie in der Liste der Serverkonfigurationen im Serverfenster folgende Anzeige: `StarDraw (Administrator).`

Manchmal verfügt ein Benutzer über mehrere Benutzernamen. Beispielsweise muss sich ein QA-Teamleiter möglicherweise als einzelner Benutzer und als QA-Teamleiter anmelden. Wenn Sie bereits bei einer Serverkonfiguration angemeldet sind oder die Anwendung Toolbar-Dienstprogramm ausgeführt wird, können Sie sich bei Bedarf unter einem anderen Benutzernamen anmelden.

Wenn Sie bereits angemeldet sind, wird der zuletzt verwendete Benutzername in den Cross-Platform Client-Dialogfeldern "Assistent für neue Projekte" und "Assistent zum Öffnen von Projekten" in Klammern hinter dem Servernamen angezeigt. Diese Informationen werden ebenfalls im Serveradministrations-Tool angezeigt.

Der in der Toolbar-Dienstprogramm in Klammern angezeigte Benutzername wird als Standardanmeldeinformation erkannt.

Hinweis: Der Server muss aktiv sein, damit diese Operation ausgeführt werden kann.

So melden Sie sich bei einer Serverkonfiguration als ein anderer Benutzer an

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.

2 Wählen Sie die Serverkonfiguration aus, auf die zugegriffen werden soll.

3 Wählen Sie im Hauptmenü **Aktionen** ▸ **Anmeldung als**. Das Dialogfeld **Bei <Serverkonfiguration> anmelden** wird angezeigt.

4 Geben Sie in die entsprechenden Textfelder einen alternativen Benutzernamen und ein Passwort ein.

5 (Optional nur für das clientseitig installierte Serveradministrations-Tool) Aktivieren Sie **Als Standard-Anmeldeinformationen für diesen Server speichern**, wenn Sie den gerade eingegebenen Benutzernamen und das entsprechende Passwort als Standardanmeldeinformationen für diese Serverkonfiguration festlegen möchten.

6 Klicken Sie auf **OK**.

Verwandte Konzepte

Richtlinien für die Serverkonfiguration
Übersicht über die Serverkonfiguration

Verwandte Verfahrensweisen

Mit Serverkonfigurationen arbeiten
Serveradministrations-Tool öffnen
Serverkonfigurationsoptionen ändern

Verwandte Referenz

Symbole für den Serverkonfigurationsstatus

Dateirevisionen mit Vault Verify verifizieren

Das Vault Verify-Dienstprogramm wird auf einem Windows-System standardmäßig im Ordner `C:\Programme \Borland\StarTeam Server 2009\VaultVerify` installiert.

Im Allgemeinen können Sie Vault Verify von der Befehlszeile aus wie folgt aufrufen: `Vault Verify [Optionen] "Serverkonfiguration"`.

So führen Sie Vault Verify aus

1 Öffnen Sie das Serveradministrations-Tool und fahren Sie die Serverkonfiguration herunter, die Sie überprüfen möchten.

Sie können die angegebene StarTeam-Konfiguration verwenden, wenn Vault Verify ausgeführt wird.

Hinweis: Die `stray`-Überprüfung und die `repair`-Option werden ignoriert, wenn die Serverkonfiguration in Gebrauch ist.

2 Navigieren Sie in der Befehlszeile zum Ordner `VaultVerify` und geben Sie folgenden Befehl ein:

```
VaultVerify.bat -check all -cf
C:\test -path "C:\Programme\Borland\StarTeam Server 2009" "Meine Serverkonfiguration"
```

Geben Sie auf einem Windows Server 2008-Rechner den folgenden Befehl ein:

```
VaultVerify.bat -check all -cf C:\test -dbname <Datenbankname>  -dbuser
<Datenbankbenutzer>  -dbinstance <Instanzname> -dbhost <Hostname>  "Meine
Serverkonfiguration"
```

Tipp: Wenn Sie Befehlszeilenoptionen für den Befehl `VaultVerify` anzeigen möchten, gehen Sie zu dem Ordner `VaultVerify` und geben Sie `VaultVerify.bat - help` ein. Sie können optional `-?` oder `-h` anstelle von `-help` verwenden.

Verwandte Konzepte

Vault Verify zum Verifizieren von Dateirevisionen

Datenbankinformationen exportieren

Mit dem Dienstprogramm für den Katalogexport werden zwei Tabellen als kommagetrennte Dateien exportiert, `Catalog_Tables` und `Catalog_Fields`. Dieses Tool ist sehr nützlich für Datenbankadministratoren, da der Katalogexport Datenbanktabellen und Spaltennamen in Bezeichner umwandelt, die vom Server verwendet werden. Exportierte Daten können in jeder Anwendung, die kommagetrennte Felder unterstützt, importiert und angezeigt werden. Wenn Sie die Datei beispielsweise mit einer .csv-Erweiterung speichern, können Sie sie in Microsoft Excel öffnen.

Wenn Sie eine Datenspalte im exportierten Feldkatalog untersuchen und feststellen, dass einer der Datensätze einen unerwarteten Wert hat (wenn z. B. alle andere Datensätze der Spalte den Wert "-1" haben, dieser Datensatz aber eine 16-stellige Zahl hat), ist dieser möglicherweise beschädigt. Borland empfiehlt jedoch nicht, dass Sie Datensätze löschen, vor allem, wenn Sie die Datenbank nicht gesichert haben.

Hinweis: Diese Operation kann nur bei deaktivierter Serverkonfiguration ausgeführt werden.

So führen Sie den Katalogexport durch

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool.

   Hinweis: Serveradministrations-Tool muss auf dem Computer gestartet werden, auf dem der Server installiert ist.

2. Wählen Sie die zu ändernde Serverkonfiguration aus und fahren Sie sie herunter.
3. Klicken Sie auf den Symbolleistenschalter **Katalogexport** oder wählen Sie im Hauptmenü **Aktionen ▸ Katalogexport**. Das Dialogfeld **Katalogexport** wird geöffnet.
4. Geben Sie im Textfeld **Dateiname für den exportierten Tabellenkatalog** den Zielpfad und den Zielspeicherort für den Tabellenkatalog ein oder suchen Sie danach.
5. Geben Sie im Textfeld **Dateiname für den exportierten Feldkatalog** den Zielspeicherort und den Zielpfad für den Feldkatalog ein oder suchen Sie danach.

   Hinweis: Geben Sie die entsprechende Dateierweiterung für die Anwendung ein, in die die Dateien exportiert werden sollen. Das Dienstprogramm gibt standardmäßig eine .csv-Datei an.

6. Klicken Sie auf **OK**. Das System zeigt die folgende Meldung an: `Der Katalog wurde erfolgreich exportiert.`
7. Öffnen Sie die Dateien in der Anwendung, in die Sie die Dateien exportiert haben.

Verwandte Verfahrensweisen

Mit Serverkonfigurationen arbeiten

Datenbankinformationen prüfen

Dieses Thema enthält Informationen zur Prüfung von Datenbankinformationen in den folgenden Dialogfeldern:

- Dialogfeld **<Name der Serverkonfiguration>-Eigenschaften**
- Dialogfeld **Server konfigurieren**

So prüfen Sie Datenbankinformationen einer Serverkonfiguration im Dialogfeld "<Name der Serverkonfiguration>-Eigenschaften":

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Sie müssen das Serveradministrations-Tool auf dem Computer verwenden, auf dem der StarTeam-Server installiert ist.
2. Wählen Sie die zu prüfende lokale Serverkonfiguration in der Serverliste aus.
3. Klicken Sie auf den Symbolleistenschalter **Konfigurationseigenschaften** oder wählen Sie **Server ▸ Konfigurationseigenschaften** im Hauptmenü. Das Dialogfeld **<Name der Serverkonfiguration>-Eigenschaften** wird geöffnet.
4. Wählen Sie das Register **Informationen zur Datenbankverbindung** , um den Datenbanktyp, ODBC-Datenbanknamen und Benutzernamen anzuzeigen.

   Tipp: Wenn die Serverkonfiguration deaktiviert ist, können Sie die Felder **ODBC-Datenbankname**, **Benutzername** und **Passwort** bearbeiten. Klicken Sie auf **Verbindung überprüfen** , um zu prüfen, ob mit diesen Angaben eine Verbindung zur Datenbank hergestellt werden kann.

5. (Nur für Serverkonfigurationen mit MS SQL-Server- oder SSE- Datenbanken) Wählen Sie das Register **Datendateien und Transaktionsprotokolle**. Die Größe und der Speicherort für Daten- und Transaktionsprotokolldateien der von dieser Serverkonfiguration verwendeten Datenbank werden angezeigt.
6. (Nur für Serverkonfigurationen mit Oracle-Datenbanken) Wählen Sie das Register **Tablespace-Informationen**.
7. Wenn Sie mit der Prüfung der Informationen fertig sind, klicken Sie auf **OK** , um das Dialogfeld zu schließen.

So prüfen Sie Datenbankinformationen einer Serverkonfiguration im Dialogfeld "Server konfigurieren":

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool. Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.
2. Wählen Sie die zu ändernde Serverkonfiguration in der Serverliste aus. Der StarTeam-Server muss aktiv sein. Wenn Sie sich bisher nicht angemeldet haben, werden Sie jetzt aufgefordert, dies zu tun.
3. Klicken Sie auf die Verknüpfung **Server konfigurieren** im unteren linken Teilfenster oder wählen Sie im Hauptmenü **Tools ▸ Administration ▸ Server konfigurieren**. Das Dialogfeld **Server konfigurieren** wird geöffnet.
4. Wählen Sie das Register **Datenbank**. Dieses Register zeigt den Datenbanktyp und den DSN-Namen an. Sie können diese Informationen nicht ändern.

Verwandte Verfahrensweisen

Serveradministrations-Tool öffnen
Serverkonfigurationen starten und stoppen
Serverkonfigurationsoptionen ändern

Verwandte Referenz

Dialogfeld 'Server konfigurieren' (Register 'Datenbank')

Erweiterte Ansichtstypen aktivieren

Standardmäßig stehen erweiterte Ansichtstypen nicht für Serverkonfigurationen zur Verfügung. Allerdings können Sie Benutzern das Erstellen von Ansichten mit erweiterten Typen ermöglichen, indem Sie die Datei `starteam-server-configs.xml` bearbeiten.

So aktivieren Sie erweiterte Ansichtstypen

1. Öffnen Sie die Datei `starteam-server-configs.xml` in einem Editor. Standardmäßig befindet sich diese Datei im Stamminstallationsordner des StarTeam-Servers. Auf einem Windows-System finden Sie diese Datei beispielsweise im Ordner `C:\Programme\Borland\StarTeam Server 2009`.
2. Geben Sie für jede Serverkonfiguration, für die erweiterte Ansichtstypen zur Verfügung stehen sollen, Folgendes ein:

   ```
   <option name="DisableAdvancedViews" value=""/>
   ```

   Wenn Sie für `value` den Eintrag `""` verwenden, wird das Auswahlfeld **Erweiterte Typen anzeigen** im **Assistent für neue Ansicht** angezeigt und die Ansichtstypen **Alle verzweigen, unverankert**, **Nicht verzweigen** und **Nicht abgeleitet** stehen im Experten zur Verfügung. Wenn Sie für `value` `"1"` angeben, wird das Auswahlfeld **Erweiterte Typen anzeigen** nicht angezeigt.

Verwandte Verfahrensweisen

Mit Serverkonfigurationen arbeiten

Gelöschte Ansichten aus Serverkonfigurationen entfernen

Dieses Thema beschreibt, wie Sie gelöschte Ansichten aus der Serverkonfiguration enfernen können, wenn der Server heruntergefahren ist. Dies wird als Offline-Bereinigung bezeichnet. Sie können die Befehlszeile oder das Serveradministrations-Tool verwenden. Durch Klicken auf den Schalter **Bereinigen** im Serveradministrations-Tool können Administratoren gelöschte Ansichten aus der Datenbank einer Serverkonfiguration und aus dem Datenspeicher entfernen und die Indizes der Datenbank neu aufbauen. Wenn die gelöschte Ansicht Elemente enthält, die in einer anderen Ansicht aktiv sind, werden diese Elemente nicht gelöscht. Wenn eine Datei beispielsweise in zwei Ansichten gemeinsam genutzt und die eine Ansicht gelöscht wird, bleibt die gemeinsam genutzte Datei erhalten. Borland empfiehlt, eine Bereinigung durchzuführen, nachdem Sie Ansichten aus einem Projekt gelöscht haben. Der Bereinigungsvorgang dauert möglicherweise mehrere Stunden, wenn eine große Anzahl von Datensätzen gelöscht oder verschoben werden muss.

Sie können Serverkonfigurationen über die Befehlszeile oder unter Verwendung von Serveradministrations-Tool dauerhaft entfernen. Es wird jedoch empfohlen, die Bereinigung mithilfe des Befehlszeilen-Tools durchzuführen. In der Regel verwenden Sie den Befehl in einer Batch-Datei (.bat) und planen die Ausführung der Batch-Datei zu einem Zeitpunkt, zu dem die Serverkonfiguration nicht aktiv ist. Da es nicht möglich ist, eine gelöschte Ansicht wiederherzustellen, wird empfohlen, das Projekt mithilfe von Zugriffsrechten für eine kurze Zeit auszublenden, bevor Sie es löschen. Wenn Sie außerdem mit großen Projekten arbeiten und die Ausfallzeiten begrenzt sind, ist es empfehlenswert, ein Projekt zunächst zu löschen und anschließend zu bereinigen, bevor Sie das nächste Projekt löschen.

Hinweis: Vor dem Bereinigungsvorgang sollten Sie zunächst ein Backup der Datenbank erstellen. Außerdem sollten Sie die Serverkonfiguration, in der die Ansicht gelöscht wurde, vor dem Bereinigen mindestens ein Mal starten. Die Bereinigungsfunktion ist für Oracle- und Microsoft SQL Server-Datenbanken verfügbar. Die Datenbank-Client-Anwendung muss auf demselben Computer wie der Server installiert sein, damit der Bereinigungsvorgang ordnungsgemäß ausgeführt wird.

Diese Operation kann nur bei deaktivierter Serverkonfiguration ausgeführt werden.

So bereinigen Sie gelöschte Ansichten unter Verwendung der Befehlszeile

1. Navigieren Sie zum Installationsordner des Servers.

   Beispiel: `C:\Programme\Borland\StarTeam Server`.

   Hinweis: Der Bereinigungsbefehl muss über den Installationsordner des Servers ausgeführt werden.

2. Geben Sie `StarTeamPurge <server_configuration_name>` in der Befehlszeile ein.

   Wenn Sie beispielsweise gelöschte Ansichten aus dem Beispielprojekt *StarDraw* bereinigen möchten, geben Sie Folgendes ein: `StarTeamPurge StarDraw`.

So bereinigen Sie gelöschte Ansichten mit dem Serveradministrations-Tool

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool.

   Hinweis: Serveradministrations-Tool muss auf dem Computer gestartet werden, auf dem der Server installiert ist.

2. Wählen Sie die zu ändernde Serverkonfiguration aus und fahren Sie sie herunter.
3. Wählen Sie die zu bereinigende Serverkonfiguration erneut aus.

4 Klicken Sie auf die Schaltfläche **Bereinigen** in der oberen Symbolleiste oder wählen Sie **Aktionen ▸ Bereinigen** aus dem Hauptmenü. Wenn Sie dazu aufgefordert werden, geben Sie Ihren Benutzernamen und das Passwort ein, um sich bei der Datenbank anzumelden.

Verwandte Konzepte

StarDraw (Beispiel-Serverkonfiguration)

Verwandte Verfahrensweisen

Mit Serverkonfigurationen arbeiten

Online-Bereinigen starten und stoppen

Dieses Thema beschreibt, wie Sie gelöschte Ansichten bei laufendem Server aus der Serverkonfiguration enfernen können. Dies wird als Online-Bereinigung bezeichnet. Um die Online-Bereinigung verwenden zu können, muss es bereits Daten geben, die aus einer oder mehreren Ansichten gelöscht wurden. Die Online-Bereinigung entfernt nur Daten, die vom Server gelöscht wurden.

Die Online-Bereinigung wird vom Serveradministrations-Tool gestartet und gestoppt. Das Register **Online-Bereinigung** im Serveradministrations-Tool ermöglicht Anwendungsadministratoren das Entfernen gelöschter Ansichten aus einer Serverkonfigurationsdatenbank und einem Datenspeicher sowie den Neuaufbau der Indizes in dieser Datenbank. Wenn die gelöschte Ansicht Elemente enthält, die in einer anderen Ansicht aktiv sind, werden diese Elemente nicht gelöscht. Wenn eine Datei beispielsweise in zwei Ansichten gemeinsam genutzt und die eine Ansicht gelöscht wird, bleibt die gemeinsam genutzte Datei erhalten. Es wird empfohlen, dass Sie nach dem Löschen einer oder mehrerer Ansichten aus einem Projekt eine Bereinigung durchführen.

Der Online-Bereinigungsvorgang dauert sehr viel kürzer als eine Offline-Bereinigung, wenn eine große Anzahl von Datensätzen gelöscht oder verschoben werden muss.

Hinweis: Bevor Sie einen Bereinigungsvorgang starten, sollten Sie auf jeden Fall die Datenbank sichern, da der Vorgang nicht rückgängig gemacht werden kann. Außerdem sollten Sie die Serverkonfiguration, in der die Ansicht gelöscht wurde, vor dem Bereinigen mindestens ein Mal starten. Die Bereinigungsfunktion ist für Oracle- und Microsoft SQL Server-Datenbanken verfügbar. Die Datenbank-Client-Anwendung muss auf demselben Computer wie der Server installiert sein, damit der Bereinigungsvorgang ordnungsgemäß ausgeführt wird.

Diese Operation kann nur bei aktivierter Serverkonfiguration ausgeführt werden.

So verwenden Sie die Online-Bereinigung

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool.
2. Wählen Sie in der **Serverliste** den Server aus, der die zu bereinigenden Daten enthält.

   Hinweis: Serveradministrations-Tool muss auf dem Computer gestartet werden, auf dem der Server installiert ist.

3. Klicken Sie auf das Symbol **Online-Bereinigung** im Abschnitt **Administration** im unteren linken Bereich des **Serveradministrations**-Fensters.

   Dadurch wird das Register **Online-Bereinigung** auf der rechten Seite des **Serveradministrations**-Fensters geöffnet.

   Hinweis: Bitte beachten Sie die Informationen im oberen Bereich des Registers **Online-Bereinigung**.

4. Drücken Sie den Schalter **Start**, um die Online-Bereinigung zu starten.

   Der Schalter **Start** ist nur im **Status** "Bereit" verfügbar. Sobald die Online-Bereinigung startet, ändert sich der Schalter in einen **Stopp**-Schalter und der **Status** ändert sich in "Wird verarbeitet".

   Bei fortschreitender Online-Bereinigung wird unter dem Schalter ein Protokoll der Löschvorgänge angezeigt. Sie können das Protokoll jederzeit aktualisieren, um den aktuellen Status der Bereinigung zu sehen.

   Hinweis: Wenn der Server aus irgendeinem Grund während einer Online-Bereinigung gestoppt wird, müssen Sie den Server neu starten und die Online-Bereinigung manuell neu starten. Die Bereinigung wird von vorn gestartet.

5 Wenn Sie die Online-Bereinigung anhalten möchten, drücken Sie den **Stopp**-Schalter.

Hinweis: Beim Stoppen der Online-Bereinigung wird der Vorgang angehalten, bis Sie ihn erneut starten, indem Sie den Schalter **Start** drücken. Wenn der Server während dieser Zeit ausgeführt wurde, wird die Online-Bereinigung von der Position aus fortgesetzt, wo sie gestoppt wurde.

Ist die Online-Bereinigung abgeschlossen, ändert sich der Schalter in einen deaktivierten **Start**-Schalter und der **Status** lautet "Abgeschlossen".

Hinweis: Sie können erst dann eine weitere Online-Bereinigung auf diesem Server starten, wenn weitere Daten vom Server gelöscht wurden.

Verwandte Konzepte

Online-Bereinigung
Online-Bereinigung

Serveradministrations-Tool öffnen

Um das Serveradministrations-Tool zur Verwaltung einer Serverkonfiguration zu verwenden, benötigen Sie Administratorrechte für die Konfiguration und diese muss ausgeführt werden. Sie können das Serveradministrations-Tool über die Befehlszeile oder über das Windows-Startmenü aufrufen.

Mit dem Dienstprogramm "Serveradministration" können Sie Serverkonfigurationen verwalten, die auf dem Computer ausgeführt werden, auf dem das Dienstprogramm installiert ist, oder auf mehreren Computern, auf denen der Server ausgeführt wird. Verbindungsinformationen für Serverkonfigurationen werden in der Datei "starteam-servers.xml" gespeichert.

So öffnen Sie das Serveradministrations-Tool mithilfe des Windows-Startmenüs

1 Wählen Sie auf dem Server **Start** ▸ **Programme** ▸ **Borland StarTeam** ▸ **StarTeam Server xxxx** ▸ **StarTeam-Server**.

2 Wenn Sie das Serveradministrations-Tool mit dem Cross-Platform Client installiert haben, wählen Sie **Start** ▸ **Programme** ▸ **Borland StarTeam** ▸ **StarTeam Cross-Platform Client xxxx** ▸ **Cross-Platform Client**. Dieses Produkt ist nur bei benutzerdefinierten Installationen verfügbar.

   Die Datei `AdminTool.stjava` wird ausgeführt, wodurch das Serveradministrations-Tool geöffnet wird. Das Serveradministrations-Tool auf dem Client ähnelt dem, das Sie mit dem Server ausführen, es kann jedoch nur für die Verwaltung von Remote-Servern verwendet werden. Einige Funktionen, z. B. die Migration einer Datenbank, können nur mit dem Serveradministrations-Tool durchgeführt werden, das mit dem Server installiert wurde, und wenn der Server heruntergefahren ist.

So starten Sie das Serveradministrations-Tool über die Befehlszeile

1 Öffnen Sie ein Befehlszeilenfenster.

2 Wechseln Sie in das Verzeichnis des Servers. Beispiel: cd `C:\Programme\Borland\StarTeam Server xxxx`.

3 Geben Sie in der Befehlszeile Folgendes ein:

   `serveradmin`

   Das Serveradministrations-Tool wird geöffnet.

Verwandte Konzepte

Richtlinien für die Serverkonfiguration
Übersicht über die Serverkonfiguration

Verwandte Verfahrensweisen

Mit Serverkonfigurationen arbeiten
Serveradministrations-Tool öffnen
Serverkonfigurationsoptionen ändern

Verwandte Referenz

Symbole für den Serverkonfigurationsstatus

Serverkonfigurationen als Windows-Dienst ausführen

Sie können eine Serverkonfiguration mithilfe des Serveradministrations-Tool starten oder in der Befehlszeile den Befehl `starteamserver` eingeben. Sie können die Serverkonfiguration auch als Microsoft Windows-Dienst ausführen.

Dieses Thema enthält folgende Informationen:

- Serverkonfigurationen als Windows-Dienst ausführen
- Windows-Dienst für eine Serverkonfiguration deaktivieren
- Ursache von Fehlern bei einem Windows-Dienst für eine Serverkonfiguration erkennen

Hinweis: Wenn eine Serverkonfiguration neu erstellt wurde, müssen Sie sie einmal starten, wieder schließen und anschließend so einrichten, dass sie als Windows-Dienst ausgeführt wird.

So richten Sie eine Serverkonfiguration als Windows-Dienst ein

1. Öffnen Sie das Serveradministrations-Tool und wählen Sie im Serverfenster die Serverkonfiguration aus.

   Hinweis: Serveradministrations-Tool muss auf dem Computer gestartet werden, auf dem der Server installiert ist.

2. Wenn der Server aktiviert ist, klicken Sie in der Symbolleiste auf **Server herunterfahren** oder wählen Sie im Hauptmenü **Aktionen** ▸ **Server herunterfahren**.

   Hinweis: Eine Konfiguration kann nicht zum Ausführen als Windows-Dienst festgelegt werden, wenn der Server einen Remote-Hive enthält, der ein zugeordnetes Laufwerk verwendet.

3. Klicken Sie in der Symbolleiste auf **Als Dienst ausführen** oder wählen Sie im Hauptmenü **Aktionen** ▸ **Als Dienst ausführen**. Das Dialogfeld **Dienst anmelden als** wird geöffnet.
4. Aktivieren Sie **Konto für lokales System**, um das lokale Konto für das System zu verwenden. Wenn Sie ein bestimmtes Benutzerkonto verwenden möchten, führen Sie folgende Schritte aus:
   1. Deaktivieren Sie das Auswahlfeld **Konto für lokales System**.
   2. Geben Sie einen Kontonamen ein. Das übliche Format ist *Domänenname\Benutzername*. Wenn das Konto zu einer integrierten Domäne gehört, können Sie .*Benutzername* verwenden.
5. Klicken Sie auf **"Anmelden"**. Es wird die Meldung angezeigt, dass der Windows-Dienst eingerichtet wurde.
6. Klicken Sie auf **OK**.

Beim nächsten Start der Serverkonfiguration oder nach einem Neustart des Computers wird die Serverkonfiguration als Windows-Dienst ausgeführt.

Wenn Sie überprüfen möchten, ob eine Serverkonfiguration als Windows-Dienst ausgeführt wird, suchen Sie den Servernamen im linken Teilfenster des Serveradministrations-Tool. Ein Symbol neben dem Namen zeigt an, ob der Server aktiviert ist und/oder als Dienst ausgeführt wird.

Wenn eine Serverkonfiguration nicht mehr als Dienst ausgeführt werden soll, müssen Sie zunächst die Serverkonfiguration anhalten und anschließend den Dienst mithilfe des Serveradministrations-Tool beenden.

So beenden Sie das Ausführen einer Serverkonfiguration als Windows-Dienst

1 Öffnen Sie das Serveradministrations-Tool und wählen Sie im Serverfenster die Serverkonfiguration aus.

Hinweis: Serveradministrations-Tool muss auf dem Computer gestartet werden, auf dem der Server installiert ist.

2 Wenn der Server aktiviert ist, klicken Sie in der Symbolleiste auf **Server herunterfahren** oder wählen Sie im Hauptmenü **Aktionen** ▸ **Server herunterfahren**.

3 Klicken Sie in der Symbolleiste auf **Als Dienst ausführen** oder wählen Sie im Hauptmenü **Aktionen** ▸ **Als Dienst ausführen**. Mit dem Symbolleistenschalter und dem Menübefehl können Sie hin- und herschalten.

Die Serverkonfiguration wird nicht mehr als Dienst ausgeführt.

Wenn eine als Dienst ausgeführte Serverkonfiguration aus irgendeinem Grund abstürzt oder heruntergefahren wird, speichert Windows diese Information im *Anwendungsprotokoll der Ereignisanzeige*.

So erkennen Sie die Ursache von Fehlern bei einem Windows-Dienst für eine Serverkonfiguration

1 Wählen Sie auf dem Computer, auf dem der Server installiert ist, im Windows-Startmenü **Einstellungen** ▸ **Systemsteuerung** ▸ **Verwaltung** ▸ **Ereignisanzeige** ▸ . Das Dialogfeld *Ereignisanzeige* wird angezeigt.

2 Klicken Sie auf den Knoten **Anwendung**. Die Protokollinformationen werden im rechten Teilfenster der Ereignisanzeige angezeigt.

3 Doppelklicken Sie auf den Protokolleintrag, um das Dialogfeld **Eigenschaften von Ereignis** anzuzeigen.

Verwandte Konzepte

Richtlinien für die Serverkonfiguration
Übersicht über die Serverkonfiguration

Verwandte Verfahrensweisen

Mit Serverkonfigurationen arbeiten
Serveradministrations-Tool öffnen
Serverkonfigurationsoptionen ändern
Serverkonfigurationen starten und stoppen

Verwandte Referenz

Symbole für den Serverkonfigurationsstatus

Serverkonfigurationen aufteilen

Das Aufteilen von StarTeam-Server-Konfigurationen wird in der Regel nicht empfohlen. Es kann allerdings sinnvoll sein, eine Serverkonfiguration aufzuteilen, wenn beispielsweise deren Größe oder deren Anzahl an aktiven Benutzern von der vorhandenen Hardware oder der Betriebssystemplattform nicht mehr bewältigt werden kann oder wenn Ihre Unternehmensprozesse vorschreiben, dass Daten von Produktionssystemen in den Archivspeicher verschoben werden müssen.

Setzen Sie sich bei Problemen hinsichtlich der Leistung oder der Skalierbarkeit mit dem Borland Technical Support in Verbindung, bevor Sie sich dazu entscheiden, Ihre StarTeam-Server-Konfiguration aufzuteilen. In vielen Fällen können die Probleme auch gelöst werden, ohne dass die Serverkonfiguration aufgeteilt werden kann.

Bevor Sie eine Serverkonfiguration aufteilen, sollten folgende Auswirkungen berücksichtigt werden.

- **Irreversibilität –** Sobald sich geteilte Serverkonfigurationen unabhängig voneinander weiterentwickeln, können sie nicht mehr zusammengeführt werden.
- **Datenabhängigkeiten –** Freigaben, Links und unverankerte Elementkonfigurationen zwischen den verschobenen und nicht verschobenen Projekten gehen verloren.
- **Administration –** Anfänglich hat eine neue Serverkonfiguration dieselbe Anzahl an Konfigurationseinstellungen, Benutzern und Gruppen wie die Originalkonfiguration. Im weiteren Verlauf müssen Sie jede Serverkonfiguration separat verwalten, da Änderungen nicht mehr untereinander weitergeleitet werden.
- **Lizenzierung –** Wenden Sie sich an den für Sie zuständigen Borland-Mitarbeiter, um mehr über potenzielle Lizenzierungsprobleme zu erfahren, die durch das Aufteilen einer Serverkonfiguration verursacht werden können. Um sicherzustellen, dass die Lizenzvereinbarung eingehalten wird, sollten Sie von einem Lizenzserver (bevorzugt FLEXlm) verwaltete Lizenzen anstatt native Lizenzen verwenden.

So teilen Sie eine StarTeam-Server-Konfiguration auf

1. Kopieren Sie die ursprüngliche Serverkonfiguration (Server 1) auf einen separaten Rechner.
2. Entfernen Sie die unerwünschten StarTeam-Projekte aus der ursprünglichen Serverkonfiguration.
3. Ordnen Sie die SQL-Server-Anmeldungen für die neue Serverkonfiguration neu zu (Server 2).
4. Ändern Sie die Server-GUID in der neuen Serverkonfiguration (Server 2).
5. Entfernen Sie die unerwünschten StarTeam-Projekte aus der neuen Serverkonfiguration (Server 2).

Hinweis: In diesem Beispiel wird vorausgesetzt, dass die ursprüngliche Serverkonfiguration (Server 1) über die drei Projekte Projekt A, Projekt B und Projekt C verfügt. Die Serverkonfiguration soll nun so aufgeteilt werden, dass Projekt A und Projekt B auf Server 1 verbleiben sollen und sich Projekt C auf der neuen Serverkonfiguration (Server 2) befinden soll.

So kopieren Sie die Konfiguration "Server 1" auf einen separaten Rechner

1. Erstellen Sie vollständige Datenbank- und Datenspeicher-Backups der Konfiguration "Server 1".
2. Stellen Sie die Datenbank und den Datenspeicher auf einem Sekundärsystem wieder her.

Warnung: Das Datenbank-Backup muss als eine andere Datenbank wiederhergestellt werden. Verwenden Sie den Datenbankspeicherort, den SQL-Server-Datenbankbenutzer oder den Oracle-Schema-Benutzer der ursprünglichen Serverkonfiguration nicht erneut.

Sobald der Kopiervorgang abgeschlossen ist, sollten Sie über zwei identische Kopien Ihrer ursprünglichen Serverkonfiguration verfügen, die auf zwei Hardware-Sets (Server und Datenbank) ausgeführt werden.

So entfernen Sie die unerwünschten StarTeam-Projekte aus der Konfiguration "Server 1"

1. Erstellen Sie vollständige Datenbank- und Datenspeicher-Backups der Konfiguration "Server 1".
2. Starten Sie die Konfiguration "Server 1".
3. Stellen Sie mit Cross-Platform Client eine Verbindung zu Server 1 her und löschen Sie "Projekt C".
4. Fahren Sie die Konfiguration "Server 1" herunter.
5. Bereinigen Sie die Konfiguration "Server 1", um die gelöschten Daten physisch zu entfernen.
6. Überprüfen Sie mit dem Vault Verify-Dienstprogramm die Integrität der Konfigurationsdaten.
7. Erstellen Sie, falls erforderlich, vollständige Datenbank- und Datenspeicher-Backups der Konfiguration "Server 1".
8. Stellen Sie die Datenbank- und Datenspeicher-Backups der Konfiguration "Server 1" von Schritt 1 auf Server 2 wieder her.
9. Wenn Sie einen anderen Speicherort für den Datenspeicher verwenden, konfigurieren Sie die Dateien `hive-index.xml` und `starteam-server-configs.xml`, damit auf den neuen Speicherort verwiesen wird.

So ordnen Sie die SQL-Server-Anmeldungen für die Konfiguration "Server 2" neu zu

1. Stellen Sie unter Verwendung von "sa" oder der Windows-Authentifizierung eine Verbindung zur Datenbank her und ändern Sie den Datenbankkontext auf die wiederhergestellte Datenbank.
2. Führen Sie den Befehl `sp_change_users_login 'REPORT'` aus. Dieser Befehl gibt den verwaisten Benutzernamen aus.

   Hinweis: Bei den folgenden Schritten wird vorausgesetzt, dass der verwaiste Benutzer `starteam` lautet. Verwenden Sie den verwaisten Benutzer, der durch den Befehl `sp_change_users_login 'REPORT'` ausgegeben wird.

3. Führen Sie die folgenden Befehle im SQL Query Analyzer aus.
   - `sp_addlogin starteam`
   - `EXEC sp_change_users_login 'Update_One', 'starteam', 'starteam'`

4. Kopieren Sie den Inhalt des Skripts `set-owner-to-dbo.sql` und führen Sie es auf die Datenbank aus.

   Hinweis: Dieses Skript befindet sich im Ordner "DBScripts" unterhalb des StarTeam-Server-Installationsverzeichnisses.

5. Führen Sie das Skript als Benutzer "sa" aus, indem Sie den Befehl `exec change_db_ownership 'starteam'` ausführen.

   Hinweis: Werden bei Ausführung des Befehls Warnhinweise ausgegeben, können diese getrost ignoriert werden.

6. Wechseln Sie zu SQL Enterprise Manager oder SQL Server Management Studio für SQL Server 2005 und löschen Sie den Benutzer `starteam` aus der Datenbank. Wählen Sie **Ja**, um auch das Schema zu löschen.

   Hinweis: Diese Aktion löscht den Datenbankbenutzer `starteam`, nicht die SQL-Server-Anmeldung `starteam`. Beim Löschen des Schemas werden alle Datenbankobjekte

gelöscht, die diesem Datenbankbenutzer gehören. Dies ist erforderlich, damit ein Datenbankbenutzer gelöscht werden kann. Dieser Schritt ist unerlässlich, da es, obwohl es viele Benutzer mit dbo-Berechtigungen geben kann, nur einen Eigentümer der Datenbank geben kann. Der StarTeam-Server muss vom Eigentümer der Datenbank ausgeführt werden.

7. Führen Sie den Befehl `sp_changedbowner starteam` aus.
8. Melden Sie sich bei der Datenbank als Benutzer "starteam" an (das Passwort ist standardmäßig leer) und führen Sie die SQL-Anweisung `select * from s0` aus.
9. Stellen Sie sicher, dass eine Zeile zurückgegeben wird.

So ändern Sie die Server-GUID in der neuen Serverkonfiguration (Server 2).

1. Ändern Sie in der Datei `starteam-server-configs.xml` die Option `ServerGuid` auf einen anderen GUID-Wert für den neuen Konfigurationsnamen. Beispiel: `<option name="ServerGuid" value="n"/>`, wobei `n` der neue Wert der Server-GUID ist.
2. Führen Sie abhängig davon, ob es sich um eine SQL-Server- oder Oracle-Datenbank handelt, einen der folgenden Schritte aus, um in der Tabelle mit den Server-Einstellungen den neuen Wert der Server-GUID anzugeben.
   - Öffnen Sie für SQL-Server eine Datenbankverbindung unter Verwendung von Microsoft SQL Server Management Studio oder Studio Express, ändern Sie den Datenbankkontext auf die neue Datenbank und führen Sie die SQL-Anweisung `update s0 set f3 = n` aus, wobei `n` der neue Wert der Server-GUID ist.
   - Öffnen Sie für Oracle unter Verwendung von SQL*Worksheet/SQL*Plus eine Datenbankverbindung zu dem neuen Schema und führen Sie die folgende SQL-Anweisung aus, wobei `n` der neue Wert der Server-GUID ist.

```
update  s0 set f3 = n;
commit;
```

So entfernen Sie die unerwünschten StarTeam-Projekte aus der neuen Serverkonfiguration (Server 2).

1. Konfigurieren Sie eine ODBC-Verbindung für die wiederhergestellte Serverkonfiguration.
2. Starten Sie die Konfiguration "Server 2".
3. Verwenden Sie Cross-Platform Client zum Verbinden mit Server 2 und löschen Sie "Projekt A" und "Projekt B".
4. Fahren Sie die Konfiguration "Server 2" herunter.
5. Bereinigen Sie die Konfiguration "Server 2", um die gelöschten Daten physisch zu entfernen.
6. Überprüfen Sie mit dem Vault Verify-Dienstprogramm die Integrität der Konfigurationsdaten.
7. Erstellen Sie, falls erforderlich, vollständige Datenbank- und Datenspeicher-Backups der Konfiguration "Server 2".

Verwandte Konzepte

Backups
Speicherorte für die Datenspeicherung

Verwandte Verfahrensweisen

Informationen sichern
Server migrieren
Serverkonfigurationen starten und stoppen
Optionen für die Datenspeicherung konfigurieren

Serverkonfigurationen deaktivieren und aktivieren

Mit dem Serveradministrations-Tool können Sie Serverkonfigurationen deaktivieren oder aktivieren. Durch das Deaktivieren einer Serverkonfiguration können Sie diese "außer Betrieb" setzen und sicherstellen, dass sie nicht versehentlich gestartet wird. Wenn Sie beispielsweise eine Serverkonfiguration migrieren, sollten Sie die alte Serverkonfiguration deaktivieren. Wenn Sie sicher sind, dass die neue Serverkonfiguration und die Datenbank ordnungsgemäß funktionieren, können Sie die alte Serverkonfiguration löschen. Sie können eine deaktivierte Serverkonfiguration außerdem reaktivieren.

Hinweis: Nur eine heruntergefahrene Serverkonfiguration kann deaktiviert bzw. aktiviert werden.

So aktivieren bzw. deaktivieren Sie eine Serverkonfiguration

1. Öffnen Sie das Serveradministrations-Tool auf dem Computer, auf dem der Server installiert ist.
2. Wählen Sie die Serverkonfiguration aus, die Sie deaktivieren bzw. aktivieren möchten, und beenden Sie sie, indem Sie auf den Symbolleistenschalter **Server herunterfahren** klicken oder im Hauptmenü **Aktionen** ▶ **Server herunterfahren** wählen.
3. Sobald der Server heruntergefahren wurde, klicken Sie auf den Symbolleistenschalter **Server deaktivieren** bzw. wählen Sie im Hauptmenü**Aktionen** ▶ **Server aktivieren**. Mit dem Symbolleistenschalter und dem Menübefehl können Sie hin- und herschalten.
   - Wenn die Serverkonfiguration aktuell aktiviert ist, wird sie deaktiviert.
   - Wenn die Serverkonfiguration aktuell deaktiviert ist, wird sie aktiviert.

Tipp: Das Symbol links neben dem Namen der Serverkonfiguration zeigt den Status an.

Verwandte Konzepte

Richtlinien für die Serverkonfiguration
Übersicht über die Serverkonfiguration

Verwandte Verfahrensweisen

Mit Serverkonfigurationen arbeiten
Serveradministrations-Tool öffnen
Serverkonfigurationsoptionen ändern

Verwandte Referenz

Symbole für den Serverkonfigurationsstatus

Serverkonfigurationen erstellen

Bevor Sie eine neue Serverkonfiguration erstellen, müssen Sie der Konfiguration einen eindeutigen Namen geben. Bei diesem Namen wird die Groß-/Kleinschreibung ignoriert. Der Name darf keine Doppelpunkte (:) sowie normale (/) oder umgekehrte (\) Schrägstriche enthalten. Leerzeichen oder Apostrophe (') sind jedoch zulässig. Außerdem müssen Sie die Datenbank einrichten, die zusammen mit dieser Serverkonfiguration verwendet werden soll. Eine Datenbank kann nur eine Serverkonfiguration enthalten, allerdings können andere Anwendungen eine Datenbank mit StarTeam gemeinsam nutzen.

Dieses Thema enthält folgende Informationen:

- Eine Serverkonfiguration mit dem Dienstprogramm Serveradministrations-Tool erstellen
- Eine Serverkonfiguration von der Befehlszeile aus erstellen

So erstellen Sie eine Serverkonfiguration

1 Öffnen Sie das Dienstprogramm Serveradministrations-Tool.

Hinweis: Serveradministrations-Tool muss auf dem Computer gestartet werden, auf dem der Server installiert ist.

2 Klicken Sie auf den Symbolleistenschalter **Neue Konfiguration** oder wählen Sie **Server** ▸ **Neue Konfiguration** im Hauptmenü. Der Experte **Neue Konfiguration erstellen** wird geöffnet.

3 Führen Sie einen der folgenden Schritte aus, um die **allgemeinen** Optionen für die neue Serverkonfiguration festzulegen:

   1 Geben Sie in das Textfeld **Konfigurationsname** einen eindeutigen Namen ein.

   2 Geben Sie in das Textfeld **Repository-Pfad** den Pfad des Speicherorts ein, an dem der Server die Serverkonfigurationsdateien erstellen soll, oder wählen Sie den Pfad aus, indem Sie auf **Durchsuchen** klicken.

   3 Wählen Sie im Listenfeld einen **Datenbanktyp** aus. Der Datenbanktyp kann nach dem Erstellen der Serverkonfiguration nicht mehr geändert werden.

   4 Aktivieren bzw. deaktivieren Sie das Auswahlfeld **Neue StarTeam-Datenbank und ODBC-Datenquelle erstellen**. Im Experten ist diese Option standardmäßig ausgewählt.

4 Wählen Sie unter **Anfängliche Hive-Einstellungen** die Hive-Option **Vorgabe** oder **Benutzerdefiniert** aus.

Hinweis: Wenn Sie die Hive-Option **Vorgabe** wählen, werden bei der Änderung des Repository-Pfads auch die vorgegebenen Hive-Einstellungen geändert. Dies ist nicht der Fall, wenn Sie die Hive-Option **Benutzerdefiniert** wählen.

Bei Auswahl der Option **Benutzerdefiniert** können Sie die folgenden vorgegebenen Hive-Einstellungen ändern:

- **Name:** Eindeutiger Name für den Hive. *DefaultHive* ist die Vorgabe.
- **Archivpfad**: Pfad zum Ordner *Archives* des neuen Hives. Die Vorgabe ist `<Repository-Pfad>\DefaultHive\Archives`.
- **Cache-Pfad**: Pfad zum Ordner *Cache* des neuen Hives. Die Vorgabe ist `<Repository-Pfad>\DefaultHive\Cache`.
- **Maximale Cache-Größe**: Die maximale Anzahl an Festplattenplatz in Megabyte, die der Cache verwenden kann. Bei aktivierter Option ist die Vorgabe 20 % des verfügbaren Speicherplatzes.

- **Cache-Cleanup-Intervall**: Sekunden zwischen den Bereinigungs- bzw. Aktualisierungsoperationen des Cache-Speichers. Der Vorgabewert ist 600. Der zulässige Bereich liegt zwischen 60 (1 Minute) und 3153600 (1 Jahr).
- **Speicherungsschwellenwert**: Prozentsatz des gesamten Speicherplatzes, der für den Hive vorgesehen ist. Wenn dieser Prozentsatz erreicht ist, fügt StarTeam dem Hive keine weiteren Archive hinzu. Der Vorgabewert beträgt 95 % des Gesamtspeicherplatzes.

5 Klicken Sie auf **Weiter**, wenn Sie alle Informationen eingegeben haben. Die zweite Seite des Experten wird geöffnet. Welche Informationen auf dieser Seite des Experten eingegeben werden müssen, hängt von der ausgewählten Datenbank ab.

Hinweis: Die ODBC-Datenquelle kann nach dem Erstellen der Serverkonfiguration nicht mehr geändert werden.

Microsoft SQL Server-/SQL Server Express-Datenbanken:

1. Wenn Sie eine auf einer SQL Server Express-Datenbank basierende Serverkonfiguration erstellen, wird im Textfeld **Host-Name** standardmäßig *(local)\SSE2005_ST* angezeigt, da die SQL Server Express-Instanz, die auf demselben Computer wie der StarTeam-Server installiert ist, den Namen *SSE2005_ST* erhalten hat. Wenn es sich um eine Microsoft SQL Server-Datenbank handelt, geben Sie den Netzwerknamen des Computers und den Namen der zu verwendenden Datenbank an.
2. Geben Sie das Passwort für den Systemadministrator in das Textfeld **Sys Admin (sa) - Passwort** ein. Wenn es sich dabei um eine SQL Server Express-Instanz handelt, ist das Standardpasswort für den Systemadministrator entweder *StarTeam123* oder *leer*.
3. Klicken Sie auf **Verbindung überprüfen**, um die Verbindung mit der Datenbank zu testen.
4. Damit der Name der Serverkonfiguration, der DSN, der Datenbankname und der Datenbank-Anmeldename gleich lauten, werden die Textfelder **ODBC-Datenquelle**, **Neuer Datenbankname** und **Neuer Datenbank-Anmeldename** auf den Namen voreingestellt, den Sie zuvor für die Serverkonfiguration auf der ersten Seite des Experten angegeben haben. Ändern Sie diese Namen bei Bedarf.
5. Geben Sie ein Datenbank-Passwort ein und bestätigen Sie es.

Oracle-Datenbanken:

1. Geben Sie den Namen des Oracle Net Service in das Textfeld **TNS-Servicename** ein.
2. Geben Sie das System-Passwort der Datenbank in das Textfeld **System-Passwort** ein.
3. Klicken Sie auf **Verbindung überprüfen**, um die Verbindung mit der Datenbank zu testen.
4. Damit der Name der Serverkonfiguration, der DSN und der Name des Schema-Benutzers gleich lauten, werden die Textfelder **Neuer Name der ODBC-Datenquelle** und **Neuer Schema-Benutzername** auf den Namen voreingestellt, den Sie zuvor für die Serverkonfiguration auf der ersten Seite des Experten angegeben haben. Ändern Sie diese Namen bei Bedarf.
5. Geben Sie ein Passwort für den Schema-Benutzernamen ein und bestätigen Sie es.

6 Klicken Sie auf **Weiter**. Die letzte Seite des Experten **Datendateien und Transaktionsprotokolle erstellen** wird geöffnet. Welche Informationen auf dieser Seite des Experten eingegeben werden müssen, hängt auch hier von der ausgewählten Datenbank ab.

Microsoft SQL Server-/SQL Server Express-Datenbanken:

1. Überprüfen Sie die im Dialogfeld angezeigten Informationen.
2. Wenn Sie über weniger als 15 Benutzer verfügen und höchstens 1 GB Daten speichern möchten, können Sie die Standardeinstellungen verwenden. Wenn Sie im Umgang mit Microsoft SQL Server- und SQL Server Express-Datenbanken sehr sicher sind, können Sie Änderungen vornehmen, nachdem Sie das

Auswahlfeld **Vorgegebene Konfiguration verwenden** deaktiviert haben. Passen Sie die Größen und Speicherorte für Daten- und Protokolldateien an. Anleitungen hierzu finden Sie unter dem Link "Richtlinien für Microsoft SQL Server-/SQL Server Express-Datendateien und -Transaktionsprotokolle" am Ende dieses Themas. Um eine Fragmentierung zu vermeiden, sollten Sie die Datendateien basierend auf der zu erwartenden maximalen Datenmenge der Datenbank so groß wie möglich machen. Verwenden Sie mindestens 3 Datendateien und mindestens 3 Transaktionsprotokolldateien beim Erstellen einer Datenbank, da Microsoft SQL Server- und SQL Server Express-Datenbanken diese proportional füllen. Auf diese Art werden alle Dateien ungefähr zur gleichen Zeit voll.

3. Wenn Sie alle Konfigurationseinstellungen festgelegt haben, klicken Sie auf **Fertig stellen**. Folgende Meldung wird angezeigt: *Stellen Sie sicher, dass der erforderliche Plattenplatz (insgesamt x MB für Daten- und Transaktionsprotokolldateien) auf dem Datenbank-Host-Computer zur Verfügung steht.*
4. Klicken Sie auf **OK**. Die Meldung *Bitte warten* wird angezeigt und automatisch ausgeblendet. Anschließend wird das Dienstprogramm Serveradministrations-Tool geöffnet, das die neue Serverkonfiguration als untergeordneten Knoten des *lokalen* Knotens anzeigt.

Hinweis: Microsoft begrenzt die Größe einer SQL Server Express-Datenbank gemäß Lizenz auf 2048 MB. Wenn Sie eine größere Datenbank benötigen, müssen Sie eine Lizenz für Microsoft SQL Server erwerben.

Oracle-Datenbanken:

1. Überprüfen Sie die im Dialogfeld angezeigten Informationen.
2. Als Tablespace-Name wird standardmäßig der Name Ihrer Serverkonfiguration angezeigt, den Sie jedoch ändern können.
3. Wenn Sie über weniger als 15 Benutzer verfügen und höchstens 1 GB Daten speichern möchten, können Sie die Standardeinstellungen verwenden. Wenn Sie mit dem Konzept der Oracle-Schema-Benutzer vertraut sind, können Sie ggf. den Namen, die Größe und den Speicherort der Datendateien ändern. Anleitungen hierzu finden Sie unter dem Link "Richtlinien für Datendateien für Oracle-Schema-Benutzer" am Ende dieses Themas. Um eine Fragmentierung zu vermeiden, sollten Sie die Datendateien basierend auf der zu erwartenden maximalen Datenmenge der Datenbank so groß wie möglich machen. Die Verwendung von mindestens drei Datendateien beim Erstellen eines Tablespace empfiehlt sich aus folgenden Gründen: Es gibt eine Größenbegrenzung von 2 GB pro Datendatei und wenn Sie weniger Dateien verwenden, kann es bei einer hohen Eingabeaktivität zu längeren Antwortzeiten kommen.
4. Klicken Sie auf **Fertig stellen**. Das Dienstprogramm Serveradministrations-Tool wird geöffnet, das die neue Serverkonfiguration als untergeordneten Knoten des *lokalen* Knotens anzeigt.

7. Wählen Sie im Serverfenster die Konfiguration aus und klicken Sie auf den Symbolleistenschalter **Server starten**. Der Server initialisiert die Datenbank und erstellt die für die Serverkonfiguration erforderlichen Dateien und Ordner.

   Der Initialisierungsvorgang dauert möglicherweise einige Minuten. Wenn der Server diese Aktion beendet hat, ändert sich das Statussymbol links neben dem Serverkonfigurationsnamen von *Neu* in *Wird ausgeführt*.

Zusätzlich zum Erstellen der Serverkonfiguration legt StarTeam Server Informationen zur neuen Serverkonfiguration in der Datei `starteam-server-configs.xml` ab.

Nach dem Erstellen der Serverkonfiguration können Sie die für die Serverkonfiguration vorgegebenen Optionen anpassen und haben somit die Möglichkeit, die Leistung Ihrer Serverkonfiguration zu optimieren.

Hinweis: Auf Betriebssystemen mit Doppelbyte-Zeichensatz (z. B. Japanisch oder Chinesisch) müssen Sie beim automatischen Erstellen eines neuen DSNs mittels StarTeam Server 2008 und einer Microsoft SQL Server 2005 SP2-Datenbank die Sortierreihenfolge manuell auf "Latin1_General_CI_AS" setzen.

So erstellen Sie eine Serverkonfiguration von der Befehlszeile aus

1 Öffnen Sie ein Fenster für die Befehlszeileneingabe und wechseln Sie zum Installationsordner des Serverprogramms.

2 Geben Sie in der Befehlszeile den folgenden Befehl ein:

```
starteamserver -new "Konfigurationsname" -r "Repository_Pfad" -t DBTyp -dsn
"Datenquellenname" -u "DBBenutzername" -p "DBBenutzerpasswort
```

Option	Beschreibung/Anmerkungen
Konfigurationsname	Ein eindeutiger Name für die Serverkonfiguration.
Repository_Pfad	Gibt den Ordner und die Dateien an, die der Server für die Serverkonfiguration erstellt. Der Server muss auf diesen Speicherort zugreifen können. Repository_Pfad darf sich nicht im Installationsordner des Servers befinden. Wenn Sie einen Repository-Pfad auswählen, der bereits von einer anderen Serverkonfiguration verwendet wurde, werden die Repository-Dateien dieser Serverkonfiguration überschrieben. Sie müssen diese Dateien manuell löschen oder verschieben, bevor Sie die neue Serverkonfiguration verwenden. Mit dem starteamserver-Befehl wird die Protokolldatei (Server.Länderkennung.Log) an diesem Speicherort abgelegt. Außerdem werden folgende Objekte unter "Repository_Pfad" angelegt: ■ Serverprotokolldateien: Bei jedem Start der Serverkonfiguration wird eine neue Serverprotokolldatei erstellt. ■ Ordner "Attachments": Der Ordner "Attachments" hat Unterordner, in denen Dateien gespeichert werden, die bestimmten Elementtypen zugeordnet sind. Der Ordner "Change_Attachments" enthält beispielsweise Dateien, die Änderungsanforderungen zugeordnet sind. Der Name dieses Ordners darf nicht geändert werden. ■ Ordner "HiveIndex": Im Ordner "HiveIndex" wird die Datei "hive-index.xml" gespeichert, die die Eigenschaften aller Hives enthält, die von der Serverkonfiguration verwendet werden. ■ Ordner "DefaultHive": Wenn Sie beim Erstellen einer Serverkonfiguration alle Vorgabe-Einstellungen akzeptieren, legt StarTeam-Server automatisch den Ordner "DefaultHive" als Unterordner von "Repository_Pfad" an. Unabhängig davon, ob der erste Hive "DefaultHive" heißt oder nicht, verfügt jede Serverkonfiguration über mindestens einen Hive. Der Hive umfasst in der Regel die zwei Unterordner "Archives" und "Cache". Sobald die Serverkonfiguration im Einsatz ist, können zusätzliche Objekte unterhalb von "Repository_Pfad" abgelegt werden.
DBTyp	Gibt den von der Serverkonfiguration verwendete Datenbanktyp an. Der Datenbanktyp kann nur beim Erstellen einer neuen Serverkonfiguration angegeben werden. Verwenden Sie zum Angeben des Datenbanktyps einen der folgenden Werte: ■ 2 = SQL Server Express oder Microsoft SQL Server ■ 3 = Oracle
Datenquellenname	ist der Datenquellenname (DSN), der für die Datenbank erstellt wird. Der Name muss im starteamserver-Befehl in doppelte Anführungszeichen (") gesetzt werden. Der DSN muss bereits vorhanden sein. In den Versionen 5.1 und 5.2 wurde auf Oracle-Datenbanken mit dem Oracle Net Service Name zugegriffen, der unter "$ORACLE_HOME/network/admin/tnsnames.ora" abgelegt ist. Dies ist nicht mehr der Fall. Erstellen Sie niemals mehrere Serverkonfigurationen, die auf dieselbe Datenbank zugreifen. Die Tabelleninformationen für eine Serverkonfiguration werden beschädigt, wenn zwei unterschiedliche Serverkonfigurationen dieselbe Datenbank aktualisieren.

DBBenutzername	Ist der Benutzername, mit dem der Server auf die Datenbank zugreift.
DBBenutzerpasswort	Ist das Passwort, mit dem der Server auf die Datenbank zugreift.

3 Der Server zeigt folgende Meldung an, wenn die Ausführung des Befehls "starteamserver" abgeschlossen ist.

Die Konfiguration Konfigurationsname wurde erfolgreich erstellt.

Das System fügt die neue Serverkonfiguration zur Datei "starteam-server-configs.xml" hinzu.

4 Sie können die Serverkonfiguration durch Eingabe des folgenden Befehls starten:

```
starteamserver -start "Konfigurationsname "
```

Wenn Sie eine neue Serverkonfiguration das erste Mal starten, führt der Server mehrere Programmstart-Aufgaben aus. Dazu gehören:

- Das Erstellen und Initialisieren der Serverkonfigurationsdatenbank.
- Das Installieren der gespeicherten Prozeduren für den angegebenen Datenbanktyp.
- Das Erstellen der Repository-Ordner.

Dieser Vorgang dauert möglicherweise einige Minuten. Wenn der Server den Vorgang beendet hat, wird folgende Meldung angezeigt:

Server Konfigurationsname erfolgreich gestartet.

Verwandte Konzepte

Richtlinien für die Serverkonfiguration
Übersicht über die Serverkonfiguration
Speicherorte für die Datenspeicherung

Verwandte Verfahrensweisen

Serveradministrations-Tool öffnen
Serverkonfigurationen starten und stoppen
Serverkonfigurationsoptionen ändern

Verwandte Referenz

Richtlinien für Microsoft SQL Server/SQL Server Express-Datendateien und -Transaktionsprotokolle
Richtlinien zu Datendateien für Oracle-Schema-Benutzer
starteam-server-configs.xml
Symbole für den Serverkonfigurationsstatus

Serverkonfigurationen sperren und entsperren

Durch das Sperren einer Serverkonfiguration kann der Zugriff auf diese während eines Backup-Vorgangs oder zu Datenbankwartungszwecken beschränkt werden. Eine gesperrte Serverkonfiguration akzeptiert nur Serveradministrationsbefehle. Bei alle anderen Vorgängen, wie z. B. dem Auschecken von Dateien, gibt der Server eine Exception-Meldung aus, dass die Serverkonfiguration nicht zur Verfügung steht.

Hinweis: Die Serverkonfiguration muss aktiv sein, damit diese Operationen ausgeführt werden können.

So sperren Sie eine Serverkonfiguration mithilfe des Serveradministrations-Tool

1. Öffnen Sie das Dienstprogramm Serveradministrations-Tool.

   Hinweis: Wenn Sie das mit dem Client installierte Serveradministrations-Tool verwenden, können Sie nur Remote-Server verwalten.

2. Wählen Sie die zu sperrende Serverkonfiguration in der Serverliste aus.
3. Klicken Sie auf das Symbol "Server sperren" in der Symbolleiste oder wählen Sie im Hauptmenü **Aktionen** ▸ **Server sperren**. Wenn Sie noch nicht bei der Serverkonfiguration angemeldet sind, müssen Sie sich anmelden.
4. Geben Sie im daraufhin angezeigten Dialogfeld an, welchen Schritt Sie ausführen möchten:
   - **Server sperren**. Wenn Sie diese Option wählen, können nur grundlegende administrative Funktionen wie das Starten, Herunterfahren, Sperren und Entsperren von Operationen ausgeführt werden. Diese Option wird in der Regel für Backup-Operationen in Umgebungen verwendet, in denen es keine 24/7-Serveraktivitäten gibt.
   - **Server exklusiv sperren für <Benutzername>**. Diese Option zeigt den Anmeldenamen des Benutzers an und ermöglicht das exklusive Sperren des Servers durch den genannten Benutzer.
5. Es wird die Meldung angezeigt, dass die Serverkonfiguration gesperrt ist. Klicken Sie auf **OK**.

Hinweis: Wenn eine gesperrte Serverkonfiguration neu gestartet wird, wird sie dadurch entsperrt.

So entsperren Sie eine gesperrte Serverkonfiguration mithilfe des Serveradministrations-Tool

1. Klicken Sie auf das Symbol **Server entsperren** in der Symbolleiste oder wählen Sie aus dem Hauptmenü **Aktionen** ▸ **Server entsperren**.
2. Es wird die Meldung angezeigt, dass die Serverkonfiguration entsperrt ist. Klicken Sie auf **OK**.

Verwandte Konzepte

- Richtlinien für die Serverkonfiguration
- Übersicht über die Serverkonfiguration

Verwandte Verfahrensweisen

- Mit Serverkonfigurationen arbeiten
- Serveradministrations-Tool öffnen
- Serverkonfigurationsoptionen ändern

Verwandte Referenz

- Symbole für den Serverkonfigurationsstatus

Serverkonfigurationen starten und stoppen

Sie können eine Serverkonfiguration mithilfe des Serveradministrations-Tool starten oder in der Befehlszeile den Befehl `starteamserver` eingeben. Sie können die Serverkonfiguration auch als Microsoft Windows-Dienst ausführen.

Dieses Thema enthält folgende Informationen:

- Serverkonfigurationen mithilfe des Serveradministrations-Tool und über die Befehlszeile starten
- Serverkonfigurationen starten, um die standardmäßigen Konfigurationsoptionen außer Kraft zu setzen: TCP/IP-Port und Pfad für Anhänge
- Serverkonfigurationen mithilfe des Serveradministrations-Tool und über die Befehlszeile stoppen

So starten Sie eine Serverkonfiguration mithilfe des Serveradministrations-Tool

1 Öffnen Sie das Dienstprogramm Serveradministrations-Tool.

Hinweis: Serveradministrations-Tool muss auf dem Computer gestartet werden, auf dem der Server installiert ist.

2 Wählen Sie die Serverkonfiguration, die Sie starten möchten, aus dem Server-Fenster aus, und führen Sie eine der folgenden Aktionen aus:

- Klicken Sie in der Symbolleiste auf **Server starten**;
- wählen Sie aus dem Hauptmenü **Aktionen** ▸ **Server starten**.

Hinweis: In beiden Fällen wird die Serverkonfiguration mit ihren standardmäßigen Konfigurationsoptionen gestartet. Der Server verwendet TCP/IP-Port 49201 als standardmäßigen Start-Port für die Serverkonfiguration.

Die Serverkonfiguration beginnt mit ihren Startoperationen. Wenn Sie eine neue Serverkonfiguration das erste Mal starten, führt der Server mehrere Programmstart-Tasks aus. Es erstellt und initialisiert die von der Serverkonfiguration verwendete Datenbank, installiert die gespeicherten Prozeduren für diesen Datenbanktyp, erstellt die Repository-Ordner und den von der Konfiguration verwendeten Hive. Dieser Vorgang dauert möglicherweise einige Minuten.

Tipp: Nachdem die Serverkonfiguration denn Startvorgang abgeschlossen hat, ändert sich das Statussymbol links neben dem Serverkonfigurationsnamen in *Wird ausgeführt*.

So starten Sie die Serverkonfiguration mit anderen Konfigurationsoptionen

1 Öffnen Sie das Serveradministrations-Tool und wählen Sie im Serverfenster die Serverkonfiguration aus.

Hinweis: Serveradministrations-Tool muss auf dem Computer gestartet werden, auf dem der Server installiert ist. Sie können auf diese Funktionalität nicht mit dem Serveradministrations-Tool zugreifen, das Sie optional mit dem Cross-Platform Client installieren können.

2 Klicken Sie in der Symbolleiste auf **Mit angepassten Serveroptionen starten** oder wählen Sie im Hauptmenü **Aktionen** ▸ **Mit angepassten Serveroptionen starten**.

Das Dialogfeld **Mit angepassten Serveroptionen starten** wird geöffnet.

3 Ändern Sie die Felder entsprechend und klicken Sie auf **OK**.

Die Serverkonfigurationsinformationen in der Datei `starteam-server-configs.xml` werden entsprechend aktualisiert. Wenn Sie den Standardendpunkt (49201) bereits für eine andere Serverkonfiguration verwenden, können Sie den Endpunkt vor dem ersten Start einer neuen Serverkonfiguration mit dieser Funktion anpassen. Der eingegebene Endpunkt wird bei allen zukünftigen Starts der Serverkonfiguration verwendet.

Sie können eine Serverkonfiguration mit den in der Datei `starteam-server-configs.xml` und in der Serverkonfigurationsdatenbank definierten Werten von der Befehlszeile aus starten oder diese Werte wie im Folgenden erläutert anpassen.

Hinweis: Mit der Option `-restart` angegebene Werte haben Vorrang vor bestimmten Serverkonfigurationswerten.

So starten Sie eine Serverkonfiguration mit definierten Werten

1. Öffnen Sie ein Fenster für die Befehlszeileneingabe und wechseln Sie zum Installationsordner des Serverprogramms.
2. Geben Sie in der Befehlszeile Folgendes ein:

```
starteamserver -start "Konfigurationsname"
```

Hinweis: Sie können auch eine Serverkonfiguration mit angepassten Werten starten, indem Sie folgenden Befehl verwenden: `starteamserver -start "Konfigurationsname" [Optionen]`.

Sie müssen eine Serverkonfiguration nicht herunterfahren, wenn Sie ein Backup durchführen möchten; für andere Wartungsaufgaben ist dies aber möglicherweise notwendig.

Hinweis: Wenn Sie eine Enterprise Advantage-Lizenz haben und den Server als Dienst sowie den Notification Agent als abhängigen Dienst ausführen, müssen Sie zunächst den Notification Agent-Dienst herunterfahren, bevor Sie die Serverkonfiguration herunterfahren können.

So fahren Sie eine Serverkonfiguration mithilfe des Serveradministrations-Tool herunter

1. Öffnen Sie das Serveradministrations-Tool und wählen Sie die Serverkonfiguration aus, die Sie herunterfahren möchten.

   Hinweis: Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.

2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie in der Symbolleiste auf **Server herunterfahren**.
   - Wählen Sie aus dem Hauptmenü **Aktionen** ▸ **Server herunterfahren**.

   Daraufhin wird das Dialogfeld **Serveradministration** geöffnet und eine Meldung angezeigt, die Sie dazu auffordert, das Herunterfahren der Serverkonfiguration zu bestätigen.

3. Klicken Sie auf **Ja** , um das Herunterfahren zu bestätigen.

So fahren Sie eine Serverkonfiguration über die Befehlszeile herunter

1. Öffnen Sie ein Fenster für die Befehlszeileneingabe und wechseln Sie zum Installationsordner des Serverprogramms.
2. Geben Sie in der Befehlszeile Folgendes ein:

```
starteamserver -stop "Konfigurationsname"
```

Verwandte Konzepte

Richtlinien für die Serverkonfiguration
Übersicht über die Serverkonfiguration

Verwandte Verfahrensweisen

Mit Serverkonfigurationen arbeiten
Serveradministrations-Tool öffnen
Serverkonfigurationsoptionen ändern
Serverkonfigurationen als Windows-Dienst ausführen

Verwandte Referenz

Symbole für den Serverkonfigurationsstatus

Serverkonfigurationsoptionen ändern

In diesem Abschnitt sind Verfahrensweisen beim Anpassen von Serverkonfigurationsoptionen beschrieben.

In diesem Abschnitt

Automatisches Wiederherstellen der Verbindung zum Server aktivieren
Beschreibt, wie Sie das Zeitlimit für Neuverbindungen für eine Serverkonfiguration aktivieren.

E-Mail-Benachrichtigungen pro Projekt und pro Komponente konfigurieren
Erklärt, wie projekt- und komponentenspezifische E-Mail-Benachrichtigungen konfiguriert werden.

E-Mail-Unterstützung und -Benachrichtigung konfigurieren
In diesem Thema wird erläutert, wie Sie E-Mail-Unterstützung und E-Mail-Benachrichtigungen für den StarTeam-Server einrichten können.

Eine Verschlüsselungsstufe festlegen
Beschreibt, wie Sie die Verschlüsselungsstufe für eine Serverkonfiguration festlegen.

Endpunkte zuweisen
Beschreibt, wie Sie den vorgegebenen TCP/IP-Port (Endpunkt) für eine Serverkonfiguration ändern.

Ereignisbehandlungen zuweisen und entfernen
Beschreibt, wie Sie Ereignisbehandlungsroutinen zu Serverkonfigurationen hinzufügen und daraus entfernen können.

Neue Ereignisbehandlungen erstellen
Beschreibt, wie Sie eine neue Ereignisbehandlungsroutine für eine Serverkonfiguration erstellen können.

Server-Zeitlimit-Optionen ändern
Beschreibt, wie Sie Server-Zeitlimit-Optionen für eine Serverkonfiguration ändern können.

Serverprobleme diagnostizieren
Beschreibt, wie Sie die Diagnosetests für eine Serverkonfiguration aktivieren.

Serversitzungsoptionen ändern
Beschreibt, wie Sie die Serversitzungsoptionen einer Serverkonfiguration ändern können.

Serverstatistik überwachen
Beschreibt, wie für eine Serverkonfiguration die Überwachung der Serverstatistik aktiviert werden kann.

Unterstützung für Verzeichnisdienst aktivieren
Beschreibt, wie Sie die Unterstützung für den Verzeichnisdienst für eine Serverkonfiguration aktivieren.

Vorhandene Ereignisbehandlungen prüfen oder ändern
Beschreibt, wie Sie vorhandene Ereignisbehandlungen für eine Serverkonfiguration prüfen oder ändern.

Automatisches Wiederherstellen der Verbindung zum Server aktivieren

Wenn ein Client seine Netzwerkverbindung verliert, wird die Verbindung der Benutzer mit dem Server unterbrochen. Mithilfe der Option "Zeitlimit für Neuverbindung" wird die Zeitspanne festgelegt, während der der Client die Verbindung erneut herstellen muss. Der Client versucht, die Verbindung nur dann wiederherzustellen, wenn der Benutzer versucht, einen Befehl an den Server zu senden. Eine erneut hergestellte Verbindung verfügt über den vollständigen Kontext der verlorenen Verbindung. Wenn der Client die Verbindung mit dem Server während des unter **Zeitlimit für Neuverbindung** eingestellten Zeitlimits erfolgreich wiederherstellt, können Benutzer einfach mit Ihrer Arbeit im Programm fortfahren. Sie müssen nicht ihre Projekte schließen, sich erneut anmelden und ihre Ansichtseinstellungen wiederherstellen.

Hinweis: Sie können das Zeitlimit für Neuverbindungen für laufende Serverkonfigurationen ändern. Dies ist nicht möglich, wenn der Server neu gestartet wurde.

Wenn der Server neu gestartet werden muss, kann der Client die Verbindung zum Server nicht automatisch wiederherstellen. Wenn Sie außerdem die Optionen **Zeitlimit für Neuverbindung** und **Zeitlimit für Inaktivität** aktiviert haben und das **Zeitlimit für Inaktivität** kürzer ist, wird der Benutzer abgemeldet, bevor der Client die Verbindung wiederherstellen kann.

So ändern Sie das Zeitlimit für Neuverbindungen

1. Öffnen Sie das Serveradministrations-Tool und wählen Sie die Serverkonfiguration aus, die Sie ändern möchten.

   Hinweis: Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.

2. Klicken Sie auf die Verknüpfung **Server konfigurieren** im Verknüpfungsfenster oder wählen Sie im Hauptmenü **Tools** ▸ **Administration** ▸ **Server konfigurieren**.

   Das Dialogfeld **Server konfigurieren** wird geöffnet.
3. Klicken Sie auf das Register **Allgemein**.
4. Aktivieren Sie das Auswahlfeld **Zeitlimit für Neuverbindung**.
5. Geben Sie eine Anzahl von Minuten in das Textfeld ein, um den Wert für das **Zeitlimit für die Neuverbindung** festzulegen. Der Standardwert ist 30 Minuten.
6. Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

Verwandte Verfahrensweisen

Serverkonfigurationsoptionen ändern
Server-Zeitlimit-Optionen ändern

Verwandte Referenz

Optionen des Dialogfelds 'Server konfigurieren'

E-Mail-Benachrichtigungen pro Projekt und pro Komponente konfigurieren

Dieses Thema beschreibt, wie die projekt- und komponentenspezifische E-Mail-Benachrichtigung konfiguriert wird, wobei die Änderungsanforderungskomponente als Beispiel verwendet wird. Es wird vorausgesetzt, dass Sie die E-Mail-Unterstützung und E-Mail-Benachrichtigung bereits aktiviert haben. Weitere Informationen hierzu finden Sie unter dem Link "E-Mail-Unterstützung und -Benachrichtigung konfigurieren" am Ende dieses Themas.

So konfigurieren Sie projekt- und komponentenspezifische E-Mail-Benachrichtigungen

1. Navigieren Sie zum Ordner *Notifications*, der bei der Installation des StarTeam-Servers angelegt wurde. Der Ordner *Notifications* wird als ein Unterordner Ihrer StarTeam-Server-Installation angelegt. Standardmäßig wird der StarTeam-Server unter *C:\Programme\Borland\StarTeam Server 2009* installiert.

   Tipp: Kopieren Sie den Ordner *Notifications*, bevor Sie Änderungen vornehmen. Sie können auf diese Kopie zurückgreifen, wenn Sie unerwünschte Änderungen vorgenommen haben sollten.

2. Sie können die komponentenspezifische `*.xml`-Datei für die Komponente (Änderungsanforderung, Task, Thema, Anforderung) bearbeiten, die Sie für projektspezifische Benachrichtigungen verwenden möchten. Öffnen Sie die Datei `ChangeRequest.xml` und geben Sie die folgenden Regeln für ein bestimmtes Projekt ein:

```
<rule-list>
```

```
  <rule project="MeinProjekt" event="new" template="MeinProjekt-cr-new-txt"/>
```

```
  <rule project="MeinProjekt" event="new" template="MeinProjekt-cr-new-txt"/>
```

   Im obigen Beispiel entspricht `"MeinProjekt"` dem Projektnamen Ihres Projekts. Diese Einträge müssen den folgenden vorangestellt werden: `<rule project="*" event="new" template="cr-new-html"/>` und `<rule project="*" event="modified" template="cr-modified-html"/>`.

3. Geben Sie die Informationen zur Vorlage, die für Ihr Projekt verwendet wird, unter dem Tag `<template-list>` an. Beispiel:

```
<template-list>
  <template-id="MeinProjekt-cr-new-txt">
    <subject>New Change Request #~~ChangeNumber~~</subject>
    <body content-type>"text/plain" template-file=".\MeinProjekt-cr-new.txt"/>
  </template>
  <template-id="MyProject-cr-modified-txt">
    <subject>Modified Change Request #~~ChangeNumber~~</subject>
    <body content-type>"text/plain" template-file=".\MyProject-cr-modified.txt"/>
  </template>
```

4. Speichern Sie die Änderungen und schließen Sie die Vorlagendatei.
5. Kopieren Sie die neuen Vorlagendateien und die aktualisierte `ChangeRequest.xml`-Datei in den Ordner *Notifications* Ihres Repositorys.

Verwandte Konzepte

E-Mail-Unterstützung und angepasste E-Mail-Benachrichtigungen

Verwandte Verfahrensweisen

E-Mail-Unterstützung und -Benachrichtigung konfigurieren

E-Mail-Unterstützung und -Benachrichtigung konfigurieren

In diesem Thema wird beschrieben, wie Sie E-Mail-Unterstützung und E-Mail-Benachrichtigungen aktivieren können. Wenn die E-Mail-Unterstützung für eine Serverkonfiguration aktiviert ist, können Benutzer in StarTeam Elementeigenschaften per E-Mail an andere Benutzer versenden. E-Mails können auch empfangen werden, wenn StarTeam gerade nicht ausgeführt wird. Wenn Sie E-Mail-Benachrichtigungsmeldungen aktivieren, sendet die Anwendung E-Mails an Benutzer, sofern diese für eine Änderungsanforderung zuständig sind, wenn sich ein Feld für eine Anforderung oder einen Task ändert, für die bzw. der der Benutzer zuständig ist, oder wenn sich ein Feld für ein Thema geändert hat, für das ein Benutzer als Empfänger aufgelistet ist.

Es wird vorausgesetzt, dass das Serveradministrationsfenster geöffnet ist und dass Sie die Serverkonfiguration, die Sie ändern möchten, ausgewählt und sich bei ihr angemeldet haben. Wenn Sie den Client (nur bei benutzerdefinierten Installationen verfügbar) verwenden, können Sie Serverkonfigurationen nur remote verwalten.

Folgende Verfahrensweisen werden in diesem Thema behandelt:

- E-Mail-Unterstützung aktivieren
- E-Mail-Benachrichtigungen aktivieren

So aktivieren Sie die E-Mail-Unterstützung für eine Serverkonfiguration

1 Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie auf die Verknüpfung **Server konfigurieren** unter dem Administrationsabschnitt im unteren linken Bereich des Fensters.
   - Wählen Sie im Hauptmenü **Tools** ▸ **Administration** ▸ **Server konfigurieren**.

   Das Dialogfeld **Server konfigurieren** wird angezeigt.

2 Klicken Sie auf das Register **Allgemein**.

3 Aktivieren Sie die Option **E-Mail-Unterstützung aktivieren**.

4 Geben Sie im Textfeld **SMTP-Server** den Host-Namen für Ihren SMTP-Server ein.

   Sie können eine IP-Adresse eingeben, wenn an Ihrem Standort nur statische IP-Adressen verwendet werden. Die Anwendung basiert auf SMTP, das traditionell TCP über Port 25 verwendet. Es ist sehr weit verbreitet und ist das standardmäßige Host-to-Host-Mail-Transportprotokoll.

   Hinweis: Unter Windows wird in der Regel der Exchange-Server als SMTP-Server verwendet.

5 Geben Sie optional einen Wert in das Textfeld **TCP/IP-Endpunkt** ein, wenn Ihr SMTP-Server einen anderen Port als den Standard-Port *25* verwendet.

6 Klicken Sie auf **OK**.

So aktivieren Sie die E-Mail-Benachrichtigungen für eine Serverkonfiguration

1 Sie können die E-Mail-Unterstützung im Register **Allgemein** im Dialogfeld **Server konfigurieren** aktivieren. Details hierzu finden Sie in der oben beschriebenen Verfahrensweise.

2 Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie auf die Verknüpfung "Server konfigurieren" unter dem Administrationsabschnitt im unteren linken Teil des Fensters.

- Wählen Sie im Hauptmenü **Tools** ▸ **Administration** ▸ **Server konfigurieren**.

Das Dialogfeld **Server konfigurieren** wird angezeigt.

3 Klicken Sie auf das Register **Allgemein**.

4 Aktivieren Sie die Option **E-Mail-Benachrichtigung aktivieren**.

Verwandte Konzepte

E-Mail-Unterstützung und angepasste E-Mail-Benachrichtigungen

Verwandte Verfahrensweisen

E-Mail-Benachrichtigungen pro Projekt und pro Komponente konfigurieren

Eine Verschlüsselungsstufe festlegen

Die Verschlüsselung schützt Dateien und andere Projektinformationen vor dem Zugriff durch unautorisierte Dritte über ungeschützte Netzwerkverbindungen, z. B. über das Internet. Für die TCP/IP-Verbindungen einer Serverkonfiguration können Sie eine minimale Verschlüsselungsstufe für die IP-Adressen festlegen, die auf die Serverkonfiguration zugreifen. Sie können unterschiedliche Verschlüsselungsstufen für eine IP-Adresse, IP-Adressbereiche oder alle IP-Adressen festlegen. Dieses Thema beschreibt beide Vorgehensweisen.

Clients können die Verschlüsselungsstufe für einzelne Workstations festlegen. Benutzer müssen mindestens die minimale Verschlüsselungsstufe verwenden, die für eine Serverkonfiguration festgelegt ist.

Hinweis: Diese Operation kann nur bei gestarteter Serverkonfiguration ausgeführt werden.

So legen Sie unabhängig von der IP-Adresse die Verschlüsselungsebene für übertragene Daten fest

1. Öffnen Sie das Serveradministrations-Tool und wählen Sie die Serverkonfiguration aus, die Sie ändern möchten.

   Hinweis: Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.

2. Klicken Sie auf die Verknüpfung **Server konfigurieren** im Verknüpfungsfenster oder wählen Sie im Hauptmenü **Tools** ▸ **Administration** ▸ **Server konfigurieren**.

   Das Dialogfeld **Server konfigurieren** wird geöffnet.

3. Wählen Sie das Register **Protokoll**.
4. Wählen Sie im Listenfeld **TCP/IP-Verschlüsselungsstufen** die Option **Standard**.
5. Klicken Sie auf **Ändern**.

   Das Dialogfeld **Verschlüsselungstyp festlegen** wird geöffnet.

6. Wählen Sie den Verschlüsselungstyp aus, der bei der Serverkonfiguration für IP-Adressen verwendet werden soll, die in der Liste nicht angegeben sind.
7. Klicken Sie auf **OK**, um die Änderungen zu übernehmen und zum Register **Protokoll** zurückzukehren.
8. Klicken Sie auf **OK**.

So legen Sie eine andere Verschlüsselungsstufe für bestimmte Adressen oder Adressbereiche fest

1. Klicken Sie auf das Register **Protokoll** des Dialogfelds **Server konfigurieren** und klicken Sie dann auf **Hinzufügen**. Das Dialogfeld **Verschlüsselungstyp festlegen** wird geöffnet.
2. Geben Sie die IP-Startadresse in die Felder **IP-Startadresse** ein.
3. Geben Sie die IP-Endadresse in die Felder **IP-Endadresse** ein.
4. Wählen Sie den Verschlüsselungstyp aus, der bei der Serverkonfiguration für diese IP-Adressen verwendet werden soll.
5. Klicken Sie auf **OK**, um die Änderungen zu übernehmen und zum Register **Protokoll** zurückzukehren.
6. Klicken Sie auf **OK**.

Verwandte Verfahrensweisen

Serverkonfigurationsoptionen ändern

Verwandte Referenz

Optionen des Dialogfelds 'Server konfigurieren'

Endpunkte zuweisen

Der vorgegebene TCP/IP-Port (Endpunkt) ist 49201, Sie können jedoch einen anderen Port für eine Serverkonfiguration angeben. Falls mehrere Serverkonfigurationen auf demselben Computer gleichzeitig ausgeführt werden, müssen diese jeweils über einen eindeutigen Endpunkt (Port) verfügen. Wenn Serverkonfiguration 1 beispielsweise den Endpunkt 49201 verwendet, muss Serverkonfiguration 2 einen anderen Endpunkt verwenden. Wenn Sie versuchen, Serverkonfigurationen mit demselben Endpunkt und Computernamen auszuführen, wird nur die erste Serverkonfiguration erfolgreich gestartet. Die übrigen Serverkonfigurationen scheinen zu starten, werden aber tatsächlich vom Server ignoriert.

Hinweis: Sie können diese Option nur bei laufenden Serverkonfigurationen ändern. Starten Sie die Serverkonfiguration neu, damit die Änderungen wirksam werden.

So weisen Sie einen Endpunkt zu

1. Öffnen Sie das Serveradministrations-Tool und wählen Sie die Serverkonfiguration aus, die Sie ändern möchten.

   Hinweis: Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.

2. Klicken Sie auf die Verknüpfung **Server konfigurieren** im Verknüpfungsfenster oder wählen Sie im Hauptmenü **Tools** ▸ **Administration** ▸ **Server konfigurieren**.

   Das Dialogfeld **Server konfigurieren** wird geöffnet.

3. Wählen Sie das Register **Protokoll**.
4. Geben Sie eine Portnummer in das Textfeld **TCP/IP (Sockets)** ein, um einen anderen Port zu aktivieren.

   Die Port-Nummer muss zwischen 1023 und 65535 liegen.

5. Klicken Sie optional auf **Vorgabe**, wenn Sie die Standardeinstellung für den Endpunkt wiederherstellen möchten (49201).
6. Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

   Hinweis: Starten Sie die Serverkonfiguration neu, damit diese Einstellung wirksam wird.

Verwandte Verfahrensweisen

Serverkonfigurationsoptionen ändern

Verwandte Referenz

Optionen des Dialogfelds 'Server konfigurieren'

Ereignisbehandlungen zuweisen und entfernen

StarTeamMPX verfügt über einen Ereignis-Transmitter, der auf demselben Computer wie der Server installiert sein muss. Zusätzlich kann der Message Broker, abhängig von Ihren Erfordernissen, auf demselben oder auf einem anderen Computer installiert werden. Wenn Sie den Message Broker installieren, wird das **Unicast On-site**-Ereignis auf dem Register **Ereignisbehandlungen** des Dialogfelds **Server konfigurieren** angezeigt.

Weitere Informationen zu StarTeamMPX, seinen XML-Dateien, Eigenschaften und Werten finden Sie im *StarTeamMPX Administrator's Guide*. In diesem Thema wird beschrieben, wie Sie Ereignisbehandlungen hinzufügen und entfernen können. Die Eigenschaften oder die verschiedenen Werte, die ihnen zugewiesen werden können, werden nicht erklärt. Das Register **Ereignisbehandlungen** verfügt über eine einfache Benutzeroberfläche zum Bearbeiten der `StarTeamMPXTransmitter.XML` -Dateien.

Hinweis: Diese Operation kann nur bei einer aktiven Serverkonfiguration ausgeführt werden.

So weisen Sie dem Server und/oder Clients Standard-Ereignisbehandlungen zu

1 Wählen Sie die zu ändernde Serverkonfiguration im Serveradministrations-Tool aus.

Hinweis: Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.

2 Klicken Sie auf die Verknüpfung **Server konfigurieren** im Verknüpfungsfenster oder wählen Sie im Hauptmenü **Tools** ▸ **Administration** ▸ **Server konfigurieren**.

Das Dialogfeld **Server konfigurieren** wird geöffnet.

3 Wählen Sie das Register **Ereignisbehandlungen**.

4 Wählen Sie eine vorhandene Ereignisbehandlung aus.

5 Führen Sie mindestens einen der folgenden Schritte aus:

- Klicken Sie auf **Servervorgabe**, um das ausgewählte Profil als Serverprofil festzulegen. Vor dem Standard-Serverprofil wird ein Serversymbol angezeigt.
- Klicken Sie auf **Client-Vorgabe**, um das ausgewählte Profil als Standardprofil für Clients festzulegen. Vor dem Standard-Client-Profil wird ein grünes Häkchen angezeigt. Wenn Benutzer auf ihren Workstations Serverbeschreibungen erstellen, wird dieses Profil anfänglich als Standardprofil angezeigt. Benutzer können neben dem Standardprofil auch andere vorhandene Profile auswählen. Wenn ein Profil als Standardprofil für den Server und die Clients dient, wird nur das Serversymbol angezeigt.

6 Klicken Sie auf **OK** , damit die Änderungen wirksam werden.

Hinweis: Datei-Transmitter verwenden keine Profile. Sie kommunizieren mit dem Ereignis-Transmitter, der das Profil **Servervorgabe** verwendet.

So entfernen Sie eine Ereignisbehandlung

1 Klicken Sie auf das Register **Ereignisbehandlungen** im Dialogfeld **Server konfigurieren**.

2 Wählen Sie eine vorhandene Ereignisbehandlung aus.

3 Klicken Sie auf **Entfernen**.

Verwandte Konzepte

Wo befindet sich die Dokumentation für die einzelnen Produkte

Neue Ereignisbehandlungen erstellen

Das Register **Ereignisbehandlungen** verfügt über eine einfache Benutzeroberfläche zum Bearbeiten der `StarTeamMPXTransmitter.XML` -Dateien.

Hinweis: Diese Operation kann nur bei einer aktiven Serverkonfiguration ausgeführt werden.

So erstellen Sie neue Ereignisbehandlungen

1. Öffnen Sie das Serveradministrations-Tool und wählen Sie die Serverkonfiguration aus, die Sie ändern möchten.

   Hinweis: Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.

2. Klicken Sie auf die Verknüpfung **Server konfigurieren** im Verknüpfungsfenster oder wählen Sie im Hauptmenü **Tools ▸ Administration ▸ Server konfigurieren**.

   Das Dialogfeld **Server konfigurieren** wird geöffnet.

3. Wählen Sie das Register **Ereignisbehandlungen**.
4. Wählen Sie eine vorhandene Ereignisbehandlung aus.
5. So erstellen Sie eine vollständig neue Ereignisbehandlung

   1. Klicken Sie auf **Hinzufügen**, um ein leeres Dialogfeld **Ereignisbehandlungs-Profileigenschaften** zu öffnen.
   2. Geben Sie einen Namen und eine Beschreibung in die entsprechenden Textfelder ein.
   3. Klicken Sie auf **Hinzufügen**, um ein leeres Dialogfeld **Ereignisbehandlungseigenschaft** anzuzeigen.
   4. Geben Sie den Eigenschaftsnamen und seinen Wert in die entsprechenden Textfelder ein.
   5. Wiederholen Sie die entsprechenden Schritte, bis Sie alle erforderlichen Eigenschaften hinzugefügt haben.

6. So erstellen Sie eine neue Ereignisbehandlung auf Grundlage einer vorhandenen

   1. Wählen Sie eine vorhandene Ereignisbehandlung aus, deren Eigenschaften der benötigten Behandlungsroutine ähneln.
   2. Klicken Sie auf **Kopieren**. Im Dialogfeld **Ereignisbehandlungs-Profileigenschaften** werden die Eigenschaften der ausgewählten Ereignisbehandlung angezeigt.
   3. Ändern Sie den Namen und die Beschreibung in den entsprechenden Textfeldern.
   4. Wählen Sie weitere Eigenschaften aus und ändern Sie diese bei Bedarf.

7. Klicken Sie auf **OK**, sobald Sie fertig sind.

Verwandte Konzepte

Wo befindet sich die Dokumentation für die einzelnen Produkte

Server-Zeitlimit-Optionen ändern

In diesem Thema werden die folgenden Verfahrensweisen beschrieben:

- Zeitlimit beim Anmeldevorgang ändern
- Zeitlimit für Inaktivität ändern
- Zeitlimit für Neuverbindung ändern

So ändern Sie das Zeitlimit beim Anmeldevorgang

1 Öffnen Sie das Serveradministrations-Tool und wählen Sie die Serverkonfiguration aus, die Sie ändern möchten.

Hinweis: Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.

2 Klicken Sie auf die Verknüpfung **Server konfigurieren** im Verknüpfungsfenster oder wählen Sie **Tools** ▸ **Administration** ▸ **Server konfigurieren** im Hauptmenü.

Das Dialogfeld **Server konfigurieren** wird geöffnet.

3 Klicken Sie auf das Register **Allgemein**.

4 Geben Sie in das Textfeld **Zeitlimit beim Anmeldevorgang** die Anzahl der **Sekunden** ein, die Benutzern für die Anmeldung zur Verfügung stehen sollen.

Das Zeitlimit für die Anmeldung beträgt fünf Minuten.

5 Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

Hinweis: Diese Option steht nur bei einer gestarteten Serverkonfiguration zur Verfügung.

So legen Sie das Zeitlimit für Inaktivität für Benutzer fest

1 Öffnen Sie das Serveradministrations-Tool und wählen Sie die Serverkonfiguration aus, die Sie ändern möchten.

Hinweis: Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.

2 Klicken Sie auf die Verknüpfung **Server konfigurieren** im Verknüpfungsfenster oder wählen Sie **Tools** ▸ **Administration** ▸ **Server konfigurieren** im Hauptmenü.

Das Dialogfeld **Server konfigurieren** wird geöffnet.

3 Klicken Sie auf das Register **Allgemein**.

4 Aktivieren Sie das Auswahlfeld **Zeitlimit für Inaktivität** .

5 Geben Sie in das Textfeld **Zeitlimit für Inaktivität** die Anzahl der Minuten ein. Klicken Sie auf "OK".

6 Optional können Sie die Option **Benannte Benutzer ausschließen** aktivieren, damit benannte Benutzer (Benutzer mit einer personengebundenen Lizenz) auch dann angemeldet bleiben können, wenn sie das **Zeitlimit für Inaktivität** überschreiten.

7 Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

Hinweis: Diese Optionen stehen nur bei einer gestarteten Serverkonfiguration zur Verfügung.

So ändern Sie das Zeitlimit für Neuverbindungen

1 Öffnen Sie das Serveradministrations-Tool und wählen Sie die Serverkonfiguration aus, die Sie ändern möchten.

Hinweis: Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.

2 Klicken Sie im Verknüpfungsfenster auf die Verknüpfung **Server konfigurieren** oder wählen Sie **Tools ▸ Administration ▸ Server konfigurieren** im Hauptmenü. Das Dialogfeld **Server konfigurieren** wird geöffnet.

3 Klicken Sie auf das Register **Allgemein**.

4 Aktivieren Sie das Auswahlfeld **Zeitlimit für Neuverbindung**.

5 Geben Sie eine Anzahl von Minuten in das Textfeld ein, um den Wert für das Zeitlimit für die Neuverbindung festzulegen. Der Standardwert ist 30 Minuten.

6 Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

Verwandte Konzepte

Server-Zeitlimit-Optionen

Verwandte Verfahrensweisen

Serveradministrations-Tool öffnen
Serverkonfigurationsoptionen ändern

Verwandte Referenz

Optionen des Dialogfelds 'Server konfigurieren'

Serverprobleme diagnostizieren

Um die Zeit zu verringern, die für die Diagnose von Problemen benötigt wird, stellt das Programm Tracing- und Debugging-Tools für den Server zur Verfügung. Mit diesen Tools können Trace-Befehlsdateien und/oder Diagnosedateien (.dmp) erstellt werden. Beide Optionen sind standardmäßig deaktiviert. Wenn ein Problem auftritt, können Sie die Optionen einfach aktivieren und Dateien erstellen, die Sie prüfen oder an den Borland Support senden können.

Hinweis: Diese Operation kann nur bei gestarteter Serverkonfiguration ausgeführt werden.

So aktivieren Sie die Optionen für die Diagnose der Serverkonfiguration

1. Öffnen Sie das Serveradministrations-Tool und wählen Sie die Serverkonfiguration aus, die Sie ändern möchten.

   Hinweis: Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.

2. Klicken Sie auf die Verknüpfung **Server konfigurieren** im Verknüpfungsfenster oder wählen Sie im Hauptmenü **Tools ▸ Administration ▸ Server konfigurieren**.

   Das Dialogfeld **Server konfigurieren** wird geöffnet.

3. Wählen Sie das Register **Diagnose**.
4. So erstellen Sie `Server.trc`-Dateien:

   - Aktivieren Sie **Operationen zurückverfolgen mit einer Mindestdauer von __ Millisekunden**.
   - Wenn Sie den Standardwert von Millisekunden nicht verwenden möchten, geben Sie eine andere Zahl ein.

   Diese Option ist standardmäßig deaktiviert.

5. Zum Erstellen von `.dmp`-Diagnosedateien wählen Sie eine oder beide der folgenden Optionen:

   - Unerwartete Zustände (Serverprotokolleinträge mit Codenummer 8)
   - Fehler (Serverprotokolleinträge mit Codenummer 4).

   Diese Optionen sind standardmäßig deaktiviert.

6. Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

Hinweis: Andere Diagnosedateitypen sollten unter der Anleitung der technischen Mitarbeiter von Borland angegeben und generiert werden.

Verwandte Verfahrensweisen

[Serverkonfigurationsoptionen ändern]

Verwandte Referenz

[Optionen des Dialogfelds 'Server konfigurieren']
[Fehlerbehebung bei Problemen mit der Serverkonfiguration]

Serversitzungsoptionen ändern

Die Sitzungsoptionen für die Serverkonfigurationen werden in der Datei `starteam-server-configs.xml` gespeichert. Sie können einige dieser Optionen mithilfe des Dienstprogramms Serveradministrations-Tool oder von der Befehlszeile aus mit dem Befehl `starteamserver` ändern.

Wenn die Serverkonfiguration nicht ausgeführt wird, können Sie die folgenden Sitzungsoptionen mit dem Dienstprogramm Serveradministrations-Tool ändern. Alle vorgenommenen Änderungen sind ab dem nächsten Start der Serverkonfiguration aktiviert. Sie können außerdem einige Konfigurationsoptionen über den Symbolleistenschalter **Mit angepassten Serveroptionen starten** ändern.

- Name der Serverkonfiguration
- Pfad zur Protokolldatei
- Informationen zur Datenbankverbindung (DSN-Name, Benutzername und Passwort)

So ändern Sie die Sitzungsoptionen für eine Serverkonfiguration

1. Öffnen Sie das Serveradministrations-Tool und wählen Sie die Serverkonfiguration aus, die Sie ändern möchten.

   Hinweis: Das Serveradministrations-Tool muss auf dem Computer gestartet werden, auf dem der Server installiert ist.

2. Wenn der Server aktiviert ist, klicken Sie auf den Symbolleistenschalter **Server herunterfahren** oder wählen Sie **Aktionen ▸ Server herunterfahren** im Hauptmenü.
3. Klicken Sie auf den Symbolleistenschalter **Konfigurationseigenschaften** oder wählen Sie **Server ▸ Konfigurationseigenschaften** im Hauptmenü.

   Das Dialogfeld**Eigenschaften** für die Serverkonfiguration wird geöffnet.
4. Geben Sie zum Ändern des Namens der Serverkonfiguration in das Textfeld **Konfigurationsname** einen neuen Namen ein.
5. Führen Sie die folgenden Schritte aus, um den Pfad für die Protokolldatei zu ändern:
   1. Klicken Sie auf **Pfad ändern**.
   2. Wählen Sie einen neuen Ordner für die Serverprotokolldatei (`Server.Länderkennung.Log`) aus.
   3. Klicken Sie auf **OK**.
6. Führen Sie die folgenden Schritte aus, um den Datenbank- oder Schema-Benutzer einer Serverkonfiguration zu ändern:
   1. Klicken Sie auf das Register **Informationen zur Datenbankverbindung** .
   2. Geben Sie einen neuen DSN-Namen in das Textfeld **ODBC-Datenbankname** ein.
   3. Geben Sie einen neuen Benutzernamen und ein Passwort in die Textfelder **Benutzername** und **Benutzerpasswort** ein. Wenn die Serverkonfiguration eine Oracle-Datenbank verwendet, lauten die Namen dieser Felder **Schema-Benutzername** und **Schema-Passwort**.
   4. Klicken Sie auf **Verbindung überprüfen**, um sicherzustellen, dass mithilfe des DSN-Namens, des Benutzernamens und des Passworts eine Verbindung zur Datenbank hergestellt werden kann.
7. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** zu schließen.

8 Starten Sie die Serverkonfiguration neu, damit die Änderungen wirksam werden.

Verwandte Verfahrensweisen

Serverkonfigurationen starten und stoppen
Serveradministrations-Tool öffnen
Serverkonfigurationsoptionen ändern

Serverstatistik überwachen

Der StarTeam-Server liefert einen HTML-Bericht zum Überwachen der Serverstatistik. Dieser Bericht zeichnet die Arbeitsspeicherauslastung, die aktuell ausgeführten Befehle, die Sperrstatistik usw. auf. Standardmäßig werden Berichte im Serverinstallationsordner `Diagnostics\ServerStatisticsMonitoring` StarTeam gespeichert.

So aktivieren Sie die Überwachung der Serverstatistik

1. Öffnen Sie das Serveradministrations-Tool und wählen Sie die Serverkonfiguration aus, die Sie ändern möchten.

   Hinweis: Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.

2. Klicken Sie auf die Verknüpfung **Server konfigurieren** im Verknüpfungsfenster oder wählen Sie im Hauptmenü **Tools** ▸ **Administration** ▸ **Server konfigurieren**.

   Das Dialogfeld **Server konfigurieren** wird geöffnet.

3. Wählen Sie das Register **Diagnose**.
4. Wählen Sie **Statistiküberwachung aktivieren. Aufzeichnen alle __ Minuten** und geben Sie das Zeitintervall für das Aufzeichnen der Statistik an.

   Diese Option ist standardmäßig deaktiviert.

5. Klicken Sie auf **OK**, damit die Änderungen wirksam werden.
6. Wählen Sie **Aktionen** ▸ **Statistiküberwachung** im Hauptmenü. Der erzeugte HTML-Bericht wird in Ihrem Web-Browser angezeigt und enthält die Serverstatistik.

Hinweis: Andere Diagnosedateitypen, die im **Diagnoseregister** verfügbar sind, sollten unter der Anleitung technischer Mitarbeiter von Borland angegeben und generiert werden.

Verwandte Verfahrensweisen

Serverkonfigurationsoptionen ändern

Verwandte Referenz

Optionen des Dialogfelds 'Server konfigurieren'

Unterstützung für Verzeichnisdienst aktivieren

StarTeam ermöglicht die Passwortverifizierung mit Microsoft Active Directory. Der Active Directory-Dienst ist in Microsoft Windows Server 2003 verfügbar.

So aktivieren Sie die Unterstützung für den Verzeichnisdienst

1. Öffnen Sie das Serveradministrations-Tool und wählen Sie die Serverkonfiguration aus, die Sie ändern möchten.

   Hinweis: Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.

2. Klicken Sie auf die Verknüpfung **Server konfigurieren** im Verknüpfungsfenster oder wählen Sie im Hauptmenü **Tools** ▸ **Administration** ▸ **Server konfigurieren**.

   Das Dialogfeld **Server konfigurieren** wird geöffnet.

3. Wählen Sie das Register **Verzeichnisdienst**.
4. Aktivieren Sie **Unterstützung für Verzeichnisdienst aktivieren**. Diese Option ist standardmäßig deaktiviert.
5. Geben Sie unter **Host** den Hostnamen und eine sichere (SSL) oder nicht sichere **Port**-Nummer für den Verzeichnisserver ein. Das Serveradministrations-Tool gibt standardmäßig Port 636 an. Zum Aktivieren der Unterstützung für den Verzeichnisdienst müssen Sie beide Werte angeben.
6. Sie können optional das Auswahlfeld **Sicheren Port verwenden** aktivieren. Dies ist die empfohlene Standardeinstellung.
7. Klicken Sie auf **OK**. Das System zeigt eine Meldung an, in der Sie zum Neustarten des Servers aufgefordert werden. Der Neustart ist zum Aktivieren des Verzeichnisdienstes erforderlich.

Hinweis: Beachten Sie, dass ein Benutzer nur dann über den Verzeichnisserver authentifiziert werden kann, wenn die Option **Über Verzeichnisdienst validieren** im Register **Anmeldung** des Dialogfelds **Eigenschaften für den neuen Benutzer** oder **Benutzereigenschaften** aktiviert ist und ein **eindeutiger Name** für den Benutzer eingegeben wurde.

Verwandte Konzepte

Übersicht über Benutzer- und Gruppenkonfigurationen

Verwandte Verfahrensweisen

Benutzer einrichten
Serverkonfigurationsoptionen ändern

Verwandte Referenz

Optionen des Dialogfelds 'Server konfigurieren'

Vorhandene Ereignisbehandlungen prüfen oder ändern

Weitere Informationen zu StarTeamMPX, seinen XML-Dateien, Eigenschaften und Werten finden Sie im *StarTeamMPX Administrator's Guide*. Dieses Thema beschreibt, wie Sie vorhandene Ereignisbehandlungen für eine Serverkonfiguration prüfen oder ändern. Die Eigenschaften oder die verschiedenen Werte, die ihnen zugewiesen werden können, werden nicht erklärt. Das Register **Ereignisbehandlungen** verfügt über eine einfache Benutzeroberfläche zum Bearbeiten der `StarTeamMPXTransmitter.XML` -Dateien.

Hinweis: Diese Operation kann nur bei einer aktiven Serverkonfiguration ausgeführt werden.

So überprüfen oder ändern Sie eine vorhandene Ereignisbehandlung

1. Öffnen Sie das Serveradministrations-Tool und wählen Sie die Serverkonfiguration aus, die Sie ändern möchten.

    Hinweis: Wenn Sie den Client verwenden, können Sie nur Remote-Server verwalten.

2. Klicken Sie auf die Verknüpfung **Server konfigurieren** im Verknüpfungsfenster oder wählen Sie im Hauptmenü **Tools** ▸ **Administration** ▸ **Server konfigurieren**.

    Das Dialogfeld **Server konfigurieren** wird geöffnet.

3. Wählen Sie das Register **Ereignisbehandlungen**.
4. Wählen Sie eine vorhandene Ereignisbehandlung aus.
5. Klicken Sie auf **Ändern**.

    Das Dialogfeld **Ereignisbehandlungs-Profileigenschaften** wird geöffnet, in dem Sie die Eigenschaftseinstellungen überprüfen oder ändern und Eigenschaften hinzufügen oder entfernen können.

6. So ändern Sie eine Einstellung:
    1. Wählen Sie im Listenfeld **Profileigenschaften** die gewünschte Einstellung aus.
    2. Klicken Sie auf **Ändern**. Das Dialogfeld **Ereignisbehandlungseigenschaft** wird geöffnet.
    3. Ändern Sie den Wert.
    4. Klicken Sie auf **OK**, um die Änderungen zu übernehmen und das Dialogfeld **Ereignisbehandlungseigenschaft** zu schließen.

7. So fügen Sie eine Eigenschaft hinzu:
    1. Klicken Sie auf **Hinzufügen**. Ein leeres Dialogfeld **Ereignisbehandlungseigenschaft** wird geöffnet.
    2. Geben Sie in die entsprechenden Felder einen Eigenschaftsnamen und einen Wert ein und klicken Sie auf **OK**.

8. So entfernen Sie eine Eigenschaft:
    1. Wählen Sie im Listenfeld **Profileigenschaften** die gewünschte Einstellung aus.
    2. Klicken Sie auf **Entfernen**. Beachten Sie, dass Sie nur Profile löschen können, die aktuell nicht als Standardprofil verwendet werden.

9. Wenn Sie mit dem Prüfen und Ändern fertig sind, klicken Sie auf **OK**.

Verwandte Konzepte

Wo befindet sich die Dokumentation für die einzelnen Produkte

Optionen für die Datenspeicherung konfigurieren

In diesem Abschnitt sind Verfahrensweisen beim Konfigurieren von Datenspeicherungsoptionen beschrieben.

In diesem Abschnitt

Archivpfad anpassen

Das Ändern des Archivpfads für einen Hive wird in der Regel aufgrund eines schwerwiegenden Problems vorgenommen, z. B. im Fall eines Laufwerksausfalls. Um dabei unerwartete Ergebnisse zu vermeiden, muss mit äußerster Vorsicht vorgegangen werden.

Hinweis: Sie müssen die Serverkonfiguration neu starten, damit der neue Archivpfad wirksam wird. Das Serveradministrations-Tool speichert den neuen Pfad sofort in der Datei `hive-index.xml`. Die Änderungen werden jedoch erst dann wirksam, nachdem Sie die Serverkonfiguration neu gestartet haben.

Hinweis: Wenn Sie auf eine Remote-Serverkonfiguration zugreifen oder eine lokale Serverkonfiguration als Remote-Server hinzugefügt wurde, können Sie den Archivpfad nur aktualisieren, wenn diese Serverkonfiguration aktiviert ist. Bei lokalem Zugriff auf eine lokale Serverkonfiguration müssen Sie die Serverkonfiguration herunterfahren, bevor der Archivpfad aktualisiert werden kann.

So ändern Sie den Archivpfad bei deaktivierten Serverkonfigurationen

1. Öffnen Sie das Serveradministrations-Tool und beenden Sie die Serverkonfiguration, deren Archivpfad geändert werden soll.
2. Kopieren Sie den Ordner "Archives" in den neuen Speicherort.
3. Öffnen Sie das Dialogfeld **Hive-Manager** im Serveradministrations-Tool, indem Sie einen der folgenden Schritte ausführen:
   - Klicken Sie im Verknüpfungsfenster auf den Schalter für die Hive-Manager-Verknüpfung.
   - Wählen Sie im Hauptmenü **Tools ▸ Administration ▸ Hive-Manager**.
4. Aktualisieren Sie das Feld **Archivpfad**, das auf den neuen Speicherort des *Archivpfads* verweist.
5. Klicken Sie auf **OK**, damit die Änderungen wirksam werden. Dadurch kehren Sie zum Dialogfeld **Hive-Manager** zurück.
6. Klicken Sie auf **OK**, um zum Hauptfenster von Serveradministrations-Tool zurückzukehren.
7. Starten Sie die Serverkonfiguration erneut.

Hinweis: Wenn Ihre Serverkonfiguration bereits mehrere Hives verwendet und der Ordner *Archives* nicht schnell an seinen neuen Speicherort verschoben werden kann, können Sie verhindern, dass neue Archive zu diesem problematischen Archivpfad hinzugefügt werden, indem Sie im Dialogfeld **Hive-Eigenschaften** die Option **Neue Archive zulassen** deaktivieren. Wenn diese Option deaktiviert ist, fügt StarTeam keine neuen Archive zum Ordner *Archives* für den angegebenen Hive hinzu.

So ändern Sie den Archivpfad für eine aktivierte Serverkonfiguration

1. Öffnen Sie das Serveradministrations-Tool und wählen Sie die aktive Serverkonfiguration aus, deren Archivpfad aktualisiert werden soll.

   Hinweis: Hierbei muss es sich um eine Remote-Serverkonfiguration bzw. um eine lokale Serverkonfiguration handeln, die als Remote-Server hinzugefügt wurde. Auf Hive-Eigenschaften von lokalen Serverkonfigurationen, die lokal ausgeführt werden, kann nicht zugegriffen werden.

2 Öffnen Sie das Dialogfeld **Hive-Manager** im Serveradministrations-Tool, indem Sie einen der folgenden Schritte ausführen:

- Klicken Sie im Verknüpfungsfenster auf den Schalter für die Hive-Manager-Verknüpfung.
- Wählen Sie im Hauptmenü **Tools** ▸ **Administration** ▸ **Hive-Manager**.

3 Wählen Sie den gewünschten Hive im Dialogfeld **Hive-Manager** aus und klicken Sie auf **Eigenschaften**.

Das Dialogfeld **Hive-Eigenschaften** wird geöffnet.

4 Wenn die Serverkonfiguration einen oder mehrere andere Hives verwendet, deaktivieren Sie das Auswahlfeld **Neue Archive zulassen** im Dialogfeld **Hive-Eigenschaften**.

Die hinzugefügten oder eingecheckten Dateien werden an den anderen Hive gesendet.

5 Starten Sie die Serverkonfiguration neu.

6 Führen Sie zur entsprechenden Zeit die folgenden Schritte aus:

1 Fahren Sie die Serverkonfiguration herunter.

2 Kopieren Sie die Archivdateien an den neuen Speicherort.

3 Ändern Sie im Dialogfeld **Hive-Eigenschaften** das Feld **Archivpfad** , sodass es auf den neuen Speicherort verweist, und aktivieren Sie das Auswahlfeld **Neue Archive zulassen**.

4 Starten Sie die Serverkonfiguration neu.

Verwandte Konzepte

Übersicht über die Datenspeicherung

Verwandte Verfahrensweisen

Neue Hives erstellen
Hive-Eigenschaften anzeigen und ändern

Dateirevisionen mit Vault Verify verifizieren

Das Vault Verify-Dienstprogramm wird auf einem Windows-System standardmäßig im Ordner `C:\Programme \Borland\StarTeam Server 2009\VaultVerify` installiert.

Im Allgemeinen können Sie Vault Verify von der Befehlszeile aus wie folgt aufrufen: `Vault Verify [Optionen] "Serverkonfiguration"`.

So führen Sie Vault Verify aus

1 Öffnen Sie das Serveradministrations-Tool und fahren Sie die Serverkonfiguration herunter, die Sie überprüfen möchten.

Sie können die angegebene StarTeam-Konfiguration verwenden, wenn Vault Verify ausgeführt wird.

Hinweis: Die `stray`-Überprüfung und die `repair`-Option werden ignoriert, wenn die Serverkonfiguration in Gebrauch ist.

2 Navigieren Sie in der Befehlszeile zum Ordner `VaultVerify` und geben Sie folgenden Befehl ein:

```
VaultVerify.bat -check all -cf
C:\test -path "C:\Programme\Borland\StarTeam Server 2009" "Meine Serverkonfiguration"
```

Geben Sie auf einem Windows Server 2008-Rechner den folgenden Befehl ein:

```
VaultVerify.bat -check all -cf C:\test -dbname <Datenbankname>  -dbuser
<Datenbankbenutzer>  -dbinstance <Instanzname> -dbhost <Hostname>  "Meine
Serverkonfiguration"
```

Tipp: Wenn Sie Befehlszeilenoptionen für den Befehl `VaultVerify` anzeigen möchten, gehen Sie zu dem Ordner `VaultVerify` und geben Sie `VaultVerify.bat - help` ein. Sie können optional `-?` oder `-h` anstelle von `-help` verwenden.

Verwandte Konzepte

Vault Verify zum Verifizieren von Dateirevisionen

Hive-Eigenschaften anzeigen und ändern

In manchen Situationen ist es erforderlich, die Eigenschaften eines bestimmten Hives zu überprüfen oder dessen Einstellungen zu ändern. Sie können beispielsweise seine Ordner *Archives* und *Cache* an einen anderen Speicherort verschieben. Verwenden Sie in diesem Fall das Dialogfeld **Hive-Manager**, um die Hive-Eigenschaften anzuzeigen und anschließend den Speicherort zu ändern.

Hinweis: Wenn Sie auf eine Remote-Serverkonfiguration zugreifen oder eine lokale Serverkonfiguration als Remote-Server hinzugefügt wurde, können Sie die Hive-Eigenschaften nur anzeigen und aktualisieren, wenn diese Serverkonfiguration aktiviert ist. Bei lokalem Zugriff auf eine lokale Serverkonfiguration müssen Sie die Serverkonfiguration herunterfahren, bevor die Hive-Eigenschaften angezeigt bzw. geändert werden können.

So zeigen Sie die Hive-Eigenschaften an und ändern deren Einstellungen

1. Öffnen Sie das Serveradministrations-Tool und wählen Sie im **Serverfenster** die Serverkonfiguration aus.

   Wenn Sie sich bisher nicht angemeldet haben, fordert Sie das Serveradministrations-Tool auf, dies zu tun, bevor Sie fortfahren.

   Hinweis: Wenn Sie lokal auf eine lokale Serverkonfiguration zugreifen, müssen Sie die Serverkonfiguration herunterfahren, bevor Sie mit dem nächsten Schritt fortfahren.

2. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie im Verknüpfungsfenster auf den Schalter für die Hive-Manager-Verknüpfung.
   - Wählen Sie im Hauptmenü **Tools ▸ Administration ▸ Hive-Manager**.

   Das Dialogfeld **Hive-Manager** wird geöffnet.

3. Wählen Sie den gewünschten Hive im Dialogfeld **Hive-Manager** aus und klicken Sie auf **Eigenschaften**. Das Dialogfeld **Hive-Eigenschaften** wird geöffnet.
4. Überprüfen und ändern Sie bei Bedarf die Informationen in diesem Dialogfeld.

   Tipp: Mit Ausnahme des Felds **Name** können Sie alle Felder im Dialogfeld **Hive-Eigenschaften** bearbeiten. Informationen zu den vorgegebenen und optionalen Einstellungen der Felder finden Sie unter dem Link "Neue Hives erstellen" am Ende dieses Themas.

5. Wenn Sie alle Änderungen eingegeben haben, klicken Sie auf **OK**, um sie zu bestätigen.

   Dadurch kehren Sie zum Dialogfeld **Hive-Manager** zurück.

6. Klicken Sie auf **OK**, um zum Hauptfenster von Serveradministrations-Tool zurückzukehren.

   Hinweis: Wenn Sie lokal auf eine lokale Serverkonfiguration zugreifen, starten Sie jetzt die Serverkonfiguration neu.

Verwandte Konzepte

Übersicht über die Datenspeicherung

Verwandte Verfahrensweisen

Neue Hives erstellen
Archivpfad anpassen

Neue Hives erstellen

Im Dialogfeld "Hive-Manager" können Sie neue Hives erstellen, um den verfügbaren Speicherplatz zu erhöhen. Sie können zudem die Eigenschaften eines vorhandenen Hives anzeigen und aktualisieren.

Hinweis: Wenn Sie auf eine Remote-Serverkonfiguration zugreifen oder eine lokale Serverkonfiguration als Remote-Server hinzugefügt wurde, können Sie neue Hives nur erstellen, wenn diese Serverkonfiguration aktiviert ist. Bei lokalem Zugriff auf eine lokale Serverkonfiguration müssen Sie die Serverkonfiguration herunterfahren, bevor ein neuer Hive erstellt werden kann.

So erstellen Sie einen neuen Hive mithilfe des Hive-Managers

1. Öffnen Sie das Serveradministrations-Tool und wählen Sie im **Serverfenster** die Serverkonfiguration aus.

   Wenn Sie sich bisher nicht angemeldet haben, fordert Sie das Serveradministrations-Tool auf, dies zu tun, bevor Sie fortfahren.

   Hinweis: Wenn Sie lokal auf eine lokale Serverkonfiguration zugreifen, müssen Sie die Serverkonfiguration herunterfahren, bevor Sie mit dem nächsten Schritt fortfahren.

2. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie im Verknüpfungsfenster auf den Schalter für die Hive-Manager-Verknüpfung.
   - Wählen Sie im Hauptmenü **Tools** ▸ **Administration** ▸ **Hive-Manager**.

   Das Dialogfeld **Hive-Manager** wird geöffnet.

3. Klicken Sie im Dialogfeld **Hive-Manager** auf **Neu**.

   Das Dialogfeld **Neuer Hive** wird geöffnet.

   Hinweis: Der Speicherort der Datei `hive-index.html` , die die Eigenschaften der von der Serverkonfiguration verwendeten Hives enthält, wird oben im Dialogfeld angezeigt.

4. Geben Sie in die folgenden Felder die Informationen zum neuen Hive ein:

   - **Name:** Eindeutiger Name für den Hive. *DefaultHive* ist die Vorgabe.
   - **Archivpfad**: Pfad zum Ordner *Archives* des neuen Hives. Die Vorgabe ist `<Repository-Pfad>\DefaultHive\Archives`.
   - **Cache-Pfad**: Pfad zum Ordner *Cache* des neuen Hives. Die Vorgabe ist `<Repository-Pfad>\DefaultHive\Cache`.
   - **Maximale Cache-Größe**: Die maximale Anzahl an Festplattenplatz in Megabyte, die der *Cache* verwenden kann. Die Vorgabe ist 20 % des Gesamtspeicherplatzes. Im Serveradministrations-Tool kann der richtige Vorgabewert für die maximale Größe des Cache-Speichers ermittelt werden. Wenn Sie jedoch das Serveradministrations-Tool verwenden und das Programm nicht auf demselben Computer wie der Server ausgeführt wird, können Sie die maximale Größe nicht berechnen. Geben Sie in diesem Fall 100 MB als Standardgröße ein.
   - **Cache-Cleanup-Intervall**: Sekunden zwischen den Bereinigungs- bzw. Aktualisierungsoperationen des Cache-Speichers. Der Vorgabewert ist 600. Der zulässige Bereich liegt zwischen 60 (1 Minute) und 3153600 (1 Jahr).

- **Speicherungsschwellenwert**: Prozentsatz des gesamten Speicherplatzes, der für den Hive vorgesehen ist. Wenn dieser Prozentsatz erreicht ist, fügt StarTeam dem Hive keine weiteren Archive hinzu. Der Vorgabewert beträgt 95 % des Gesamtspeicherplatzes.

Tipp: Sie können UNC-Pfade für Archiv- und Cache-Pfade verwenden.

5 Aktivieren bzw. deaktivieren Sie die Option **Neue Archive zulassen**. Das Feld ist standardmäßig aktiviert. Wenn für diese Serverkonfiguration keine weiteren Hives existieren, muss dieses Auswahlfeld aktiviert werden.

Hinweis: Wenn Sie einen Hive hinzufügen, weil im ursprünglichen Hive nicht mehr ausreichend Speicherplatz vorhanden ist, sollten Sie mithilfe des Dialogfelds **Hive-Manager** auch die Eigenschaften des Hives überprüfen und das Auswahlfeld **Neue Archive zulassen** deaktivieren. Dadurch verbleibt der ursprüngliche Hive als Speicherort für das Auschecken, es werden aber keine neuen Dateien mehr angenommen. Hinzugefügte Dateien werden dem neuen Hive hinzugefügt.

6 Füllen Sie das Textfeld **Archivpfad des Root-Cache-Agenten** aus, wenn Sie den Cache-Agenten verwenden und der Root-Cache-Agent nicht auf demselben Computer wie der Server ausgeführt wird. Geben Sie den Cache-Pfad aus der Sicht des Cache-Agenten an.

Angenommen Sie erstellen einen neuen Hive mit dem Archivpfad `C:\ProdServer\Hives\NewHive\Archives`. Der Root-Cache-Agent wird jedoch auf einem Computer ausgeführt, auf dem `H:\` dem Verzeichnis `C:\ProdServer\Hives` auf dem StarTeam-Server zugeordnet ist. Der Root-Cache-Agent bekäme dann den Archivpfad des neuen Hives als `H:\NewHive\Archives` angezeigt. In diesem Fall würden Sie `H:\NewHive\Archives` in das Textfeld **Archivpfad des Root-Cache-Agenten** eingeben.

7 Klicken Sie auf **OK**, damit die Änderungen wirksam werden. Dadurch kehren Sie zum Dialogfeld **Hive-Manager** zurück.

8 Klicken Sie auf **OK**, um zum Hauptfenster von Serveradministrations-Tool zurückzukehren.

Hinweis: Wenn Sie lokal auf eine lokale Serverkonfiguration zugreifen, starten Sie jetzt die Serverkonfiguration neu.

Verwandte Konzepte

Übersicht über die Datenspeicherung

Verwandte Verfahrensweisen

Archivpfad anpassen
Hive-Eigenschaften anzeigen und ändern

Referenz

Dieser Abschnitt enthält Referenzthemen.

In diesem Abschnitt

Administration und Konfiguration

Dieser Abschnitt enthält Referenzthemen, die sich mit der Administration und der Konfiguration befassen.

In diesem Abschnitt

Projektstruktur

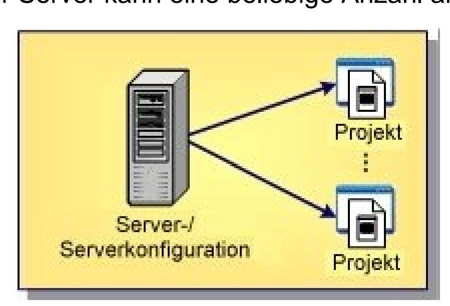
Eine Instanz des Servers verwaltet die Ablage Ihrer Dateien. Jede Serverinstanz führt eine Serverkonfiguration aus. Nachfolgend finden Sie eine Übersicht zur Projektstruktur, die von einer Serverinstanz gesteuert wird.

Server	Ein Server ist ein Computer, auf dem die Server-Software ausgeführt wird. Mit StarDisk können Sie auf den Server zugreifen. Der Server steuert das Repository, einen Speicherplatz für Dateirevisionsarchive und eine Datenbank, die Informationen zu Dateien enthält, z. B. ihre Beschreibungen, die Anzahl der Revisionen usw.
Projekt	Ein Projekt dient dazu, alle Materialien zusammenzufassen, die zum Erreichen eines Ziels erforderlich sind. Große, komplexe Projekte enthalten viele Ordner und Dateien, die von vielen Teammitgliedern bearbeitet werden. In einem Projekt sind alle diese Dateien und Ordner zusammengefasst und können organisiert werden. Ein Projekt kann die Dateien eines Software-Programms, einer technischen Publikation, eines Rechtsstreits, einer Umsatzprognose, eines Gebäudes oder eines Flugzeugs bzw. alles mögliche enthalten, was aus mehrere Dateien besteht und bei fortlaufender Arbeit mehrere Revisionen umfasst.
Ansicht	Eine Ansicht oder Projektansicht bietet eine bestimmte Sicht auf die Projektdaten. Dadurch können Benutzer die Teile des Projekts sehen, die für Sie gerade wichtig sind. Die unwichtigen Teile werden dabei ausgeblendet. Benutzer können verschiedene unterschiedliche Ansichten für ein einzelnes Projekt oder Ansichten mehrerer Projekte verwenden. Dies hängt von den verwendeten Dateien ab. Jeder Projekt hat nur eine Stammansicht, die beim Anlegen des Projekts automatisch erstellt wird. Die Stammansicht kann mehrere untergeordnete Ansichten enthalten, die selbst wiederum untergeordnete Ansichten enthalten können. Eine Ansicht mit untergeordneten Ansichten wird auch als übergeordnete Ansicht bezeichnet.
Ordner	Jede Ansicht hat einen Stammordner. Dieser Ordner kann eine beliebige Ordnerhierarchie enthalten. Die einzelnen Ordner haben Namen, die ihren Inhalt beschreiben, z. B. "Marketing Materials", "Product Documentation" und "Source Code".

Nachfolgend finden Sie einige Diagramme, die veranschaulichen, wie sich die einzelnen Teile zusammenfügen.

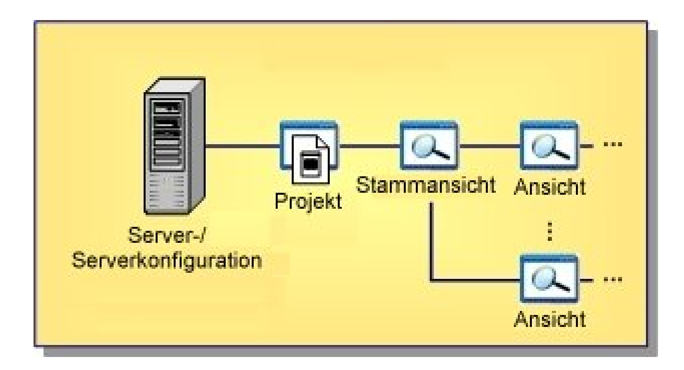
Hierarchie auf Serverebene

Der Server kann eine beliebige Anzahl an Projekten verwalten.



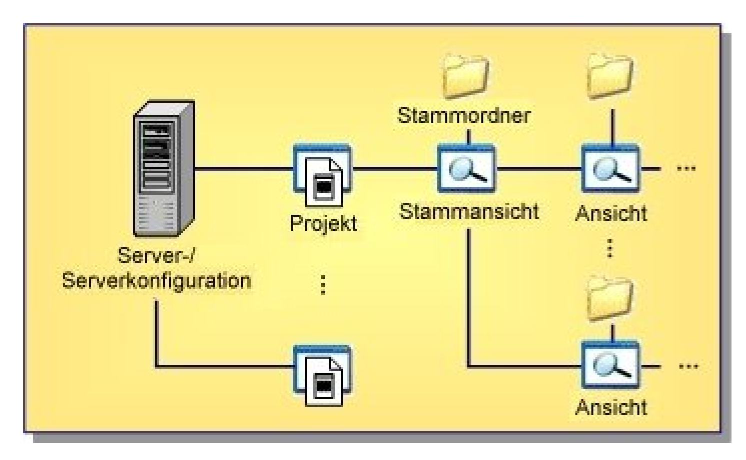
Hierarchie auf Projektebene

Jedes Projekt setzt sich aus einer Stammansicht und einer beliebigen Anzahl untergeordneter Ansichten zusammen.



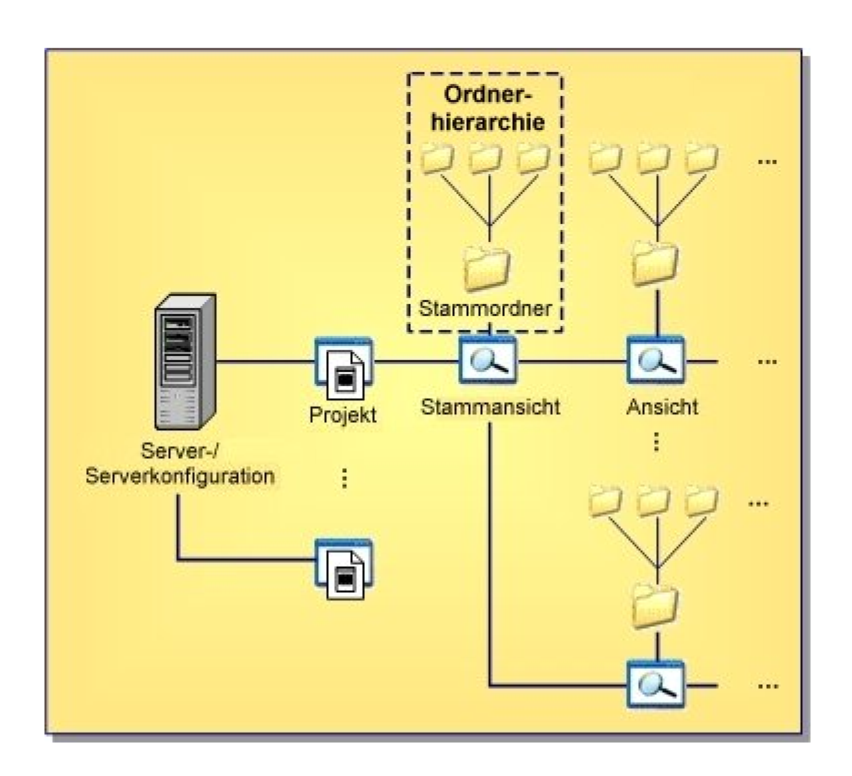
Hierarchie auf Ansichtsebene

Die Stammansicht und alle untergeordneten Ansichten verfügen über jeweils einen Anwendungsordner als Stammordner.



Hierarchie auf Ordnerebene

Jedem Stammordner einer Anwendung kann eine beliebige Hierarchie von Ordnern untergeordnet sein. Dies wird als Ordnerhierarchie bezeichnet.


Ordner-
hierarchie
Stammordner
Projekt
Stammansicht
Ansicht
Server-/
Serverkonfiguration

Optionen des Dialogfelds 'Server konfigurieren'

Dieser Abschnitt enthält Referenzthemen zum Dialogfeld **Server konfigurieren** .

In diesem Abschnitt

Dialogfeld 'Server konfigurieren' (Register 'Allgemein')

Tools ▸ Administration ▸ Server konfigurieren

Im Register **Allgemein** des Dialogfelds **Server konfigurieren** können Sie den Pfad für Anhänge bearbeiten, die Optionen für das Server-Timeout festlegen und die E-Mail-Unterstützung aktivieren.

Element	Beschreibung
Protokolldatei für den Serverstart	Der Standardwert ist `..\Repository-Pfad\server.log`. Dieses Feld ist schreibgeschützt; Pfad wird beim Erstellen einer neuen Serverkonfiguration angegeben.
Pfad für Anhänge	Der Standardwert ist `..\Repository-Pfad\Anhänge`. Dies ist ein bearbeitbarer Pfad; Ordner wird vom Server erstellt.
Zeitlimit beim Anmeldevorgang	Der Standardwert ist 60 Sekunden. Jede Anmeldung, die nicht innerhalb dieser Zeit abgeschlossen wird, schlägt fehl.
Zeitlimit für Inaktivität __ Minuten	Der Standardwert ist *Aus*. Benutzer, die über das Zeitlimit hinaus inaktiv sind, werden automatisch abgemeldet. Dies gilt jedoch nicht für Benutzer, die die Systembenachrichtigung unter **Persönliche Optionen** aufgrund der automatischen Kommunikation zwischen dem Client und dem Server auf einen kürzeren Zeitraum gesetzt haben. Auch Benutzer mit personengebundenen Lizenzen sind davon ausgenommen, wenn die Option **Benannte Benutzer ausschließen** (siehe unten) ausgewählt ist. Setzen Sie das **Zeitlimit für Inaktivität** immer auf einen höheren Wert als das **Zeitlimit für Neuverbindung**. Wenn sowohl das **Zeitlimit für Neuverbindung** als auch das **Zeitlimit für Inaktivität** aktiviert sind und das **Zeitlimit für Inaktivität** kürzer ist als das **Zeitlimit für Neuverbindung**, wird der Benutzer abgemeldet, bevor der Client die Verbindung wiederherstellen kann.
Benannte Benutzer ausschließen	Diese Option ist standardmäßig deaktiviert. Benannte Benutzer bleiben angemeldet, auch wenn sie das **Zeitlimit für Inaktivität** überschritten haben. Diese Funktion ist nur verfügbar, wenn **Zeitlimit für Inaktivität** ausgewählt und ein Wert eingegeben wird.
Zeitlimit für Neuverbindung __ Minuten	Der Standardwert ist 30 Minuten. Legt fest, über wie viel Zeit der Client verfügt, um eine unterbrochene Netzwerkverbindung mit dem Server wiederherzustellen. Der Client versucht, die Verbindung nur dann wiederherzustellen, wenn der Benutzer versucht, einen Befehl an den Server zu senden. Wenn das Zeitlimit für das Wiederherstellen der Verbindung abgelaufen ist, wird die Sitzung des Benutzers vom Server gelöscht. Der Aufbau einer neuen Verbindung kann nicht ausgeführt werden, wenn der Server neu gestartet wurde. Wenn sowohl **Zeitlimit für Neuverbindung** als auch **Zeitlimit für Inaktivität** aktiviert sind und das **Zeitlimit für Inaktivität** kürzer ist, wird der Benutzer abgemeldet, bevor der Client die Verbindung wiederherstellen kann.
E-Mail-Unterstützung aktivieren	Der Standardwert ist *Aus*. Benutzer können in der Anwendung Elemente per E-Mail an andere Benutzer senden, selbst wenn der Empfänger die Anwendung nicht

	geöffnet hat. Diese Funktion muss aktiviert sein, um die Option für die Benachrichtigung per E-Mail auswählen zu können. Wenn die E-Mail-Unterstützung aktiviert ist, muss für jeden Benutzer eine E-Mail-Adresse eingegeben werden.
SMTP-Server	Diese Option ist standardmäßig deaktiviert. Ist erforderlich, wenn die E-Mail-Unterstützung aktiviert ist.
TCP/IP-Endpunkt	Diese Option ist standardmäßig deaktiviert. Der Standard-SMTP-Port ist 25, wenn die E-Mail-Unterstützung aktiviert ist.
E-Mail-Benachrichtigung aktivieren	Der Standardwert ist *Aus*. Die Option ist verfügbar, wenn **E-Mail-Unterstützung aktivieren** ausgewählt, ein **SMTP-Server** aktiviert und für den SMTP-Server ein **Port** angegeben ist. Wenn die Benachrichtigung aktiviert ist, erhält ein Teammitglied eine E-Mail, wenn es für diese Änderungsanforderung verantwortlich ist, wenn sich ein Feld für eine Anforderung oder eine Aufgabe ändert, das in seinen Zuständigkeitsbereich fällt, oder wenn sich ein beliebiges Feld eines Themas ändert, für das der Benutzer als Empfänger registriert ist.
Erweiterte Prozess-Links für alle Projekte aktivieren	Damit wird es Benutzern ermöglicht, erweiterte Prozess-Links für alle Projekte auf der Serverkonfiguration zu aktivieren oder deaktivieren.
Erweiterte Prozess-Links für neue Projekte aktivieren	Damit wird es Benutzern ermöglicht, erweiterte Prozess-Links für neue Projekte, die auf diesem Server erstellt wurden, zu aktivieren oder deaktivieren. Beachten Sie, dass diese Option für Serverkonfigurationen, die mit einer älteren Version von StarTeam-Server erstellt wurden (vor StarTeam-Server 2008) nicht zur Verfügung steht.

Verwandte Verfahrensweisen

Automatisches Wiederherstellen der Verbindung zum Server aktivieren
E-Mail-Unterstützung und -Benachrichtigung konfigurieren
Serverkonfigurationsoptionen ändern

Verwandte Referenz

Optionen des Dialogfelds 'Server konfigurieren'

Dialogfeld 'Server konfigurieren' (Register 'Audits')

Tools ▸ Administration ▸ Server konfigurieren

Im Register **Audits** des Dialogfelds **Server konfigurieren** können Sie das Generieren und Bereinigen der Audit-Protokolle aktivieren.

Element	Beschreibung
Audit-Generierung aktivieren	Der Standardwert ist *Ein*. Audit-Protokolldaten werden in der Datenbank für die Serverkonfiguration gespeichert. Wenn die Daten zu viel Speicherplatz benötigen, kann die Option deaktiviert werden.
Audit-Einträge entfernen, die älter sind als __ Tage	Der Standardwert ist *Aus*. Um den erforderlichen Speicherplatz so niedrig wie möglich zu halten, werden alle Audit-Einträge entfernt, die älter als eine angegebene Anzahl von Tagen sind. Der Standardwert ist 90 Tage, wenn die Option aktiviert ist. Die Anzahl der Tage kann geändert werden. Die Serverkonfiguration muss zum Bereinigen der Audit-Protokolle neu gestartet werden.

Verwandte Referenz

Optionen des Dialogfelds 'Server konfigurieren'

Dialogfeld 'Server konfigurieren' (Register 'Datenbank')

Tools ▸ Administration ▸ Server konfigurieren

Im Register **Datenbank** des Dialogfelds **Server konfigurieren** können Sie den Datenbanktyp und den DSN für die Serverkonfiguration anzeigen.

Element	Beschreibung
Datenbanktyp	Nicht aktiv. Schreibgeschützt; der Typ der Datenbank kann nur beim Erstellen der Serverkonfiguration festgelegt werden.
DSN	Nicht aktiv. Schreibgeschützt; das Element kann nur beim Erstellen der Serverkonfiguration festgelegt werden.

Verwandte Verfahrensweisen

Serverkonfigurationsoptionen ändern

Verwandte Referenz

Optionen des Dialogfelds 'Server konfigurieren'

Dialogfeld 'Server konfigurieren' (Register 'Protokoll')

Tools ▸ Administration ▸ Server konfigurieren

Im Register **Protokoll** des Dialogfelds **Server konfigurieren** können Sie die standardmäßigen Endpunkte und Verschlüsselungsstufen für eine Serverkonfiguration festlegen.

Hinweis: Das Ändern der Endpunkte wirkt sich erst nach dem Neustart der Serverkonfiguration aus.

Element	Beschreibung
TCP/IP-Endpunkt	Der Standardwert 49201 wird beim Erstellen einer Serverkonfiguration ausgewählt.
TCP/IP-Verschlüsselungsstufen	Die Vorgabe ist *Keine Verschlüsselung*. Werden zum Festlegen einer Mindestverschlüsselungsstufe für Daten verwendet, die per TCP/IP übertragen werden; verwenden Sie die Schaltflächen **Hinzufügen**, **Entfernen** und **Ändern** zum Bearbeiten der Verschlüsselungsstufen.

Verwandte Referenz

Optionen des Dialogfelds 'Server konfigurieren'

Dialogfeld 'Server konfigurieren' (Register 'Ereignisbehandlungen')

Tools ▸ Administration ▸ Server konfigurieren

Im Register **Ereignisbehandlungen** des Dialogfelds **Server konfigurieren** können Sie Servern und/oder Clients standardmäßige Ereignisbehandlungen zuweisen.

Element	Beschreibung
Ereignisbehandlung	Der Standardwert ist *Kein*. Diese Option ermöglicht die Eingabe oder das Auswählen einer Ereignisbehandlungsroutine.
Beschreibung der Ereignisbehandlung	Der Standardwert ist *Ein*. Diese Option ermöglicht die Beschreibung einer ausgewählten Ereignisbehandlungsroutine.

Verwandte Referenz

Optionen des Dialogfelds 'Server konfigurieren'

Dialogfeld 'Server konfigurieren' (Register 'Verzeichnisdienst')

Tools ▸ Administration ▸ Server konfigurieren

Im Register **Verzeichnisdienst** des Dialogfelds **Server konfigurieren** können Sie die Unterstützung für den Verzeichnisdienst für die Serverkonfiguration aktivieren.

Element	Beschreibung
Unterstützung für Verzeichnisdienst aktivieren	Der Standardwert ist *Aus*. Verwendet den angegebenen Microsoft Active Directory-Dienst zum Validieren von Benutzerpasswörtern. Damit das Passwort eines Benutzers validiert werden kann, muss außerdem die Option **Verzeichnisdienst validieren** in den Dialogfeldern **Eigenschaften für den neuen Benutzer** oder **Benutzereigenschaften** aktiviert sein und es muss ein **eindeutiger Name** im Microsoft Active Directory-Dienst für den Benutzer eingegeben werden. Starten Sie die StarTeam-Serverkonfiguration neu, um sicherzugehen, dass die Verbindung zu dem Dienst aufgenommen werden kann, bevor Sie die Benutzer einrichten. Das Serverprotokoll enthält die Verbindungsinformationen, beispielsweise "Verbunden mit Active Directory Server: ldaps://host:port", wobei die Werte für den Host und den Port die in diesem Register angegebenen Werte sind.
Host	Host-Name oder IP-Adresse des Microsoft Active Directory-Dienstes; alphanumerischer Wert mit bis zu 254 Zeichen. Statt eines Host-Namens oder einer IP-Adresse können Sie im Textfeld **Host** einen Domänennamen angeben. Wenn Sie einen Domänennamen verwenden, kann der StarTeam-Server eine beliebige aktive Kopie von Active Directory von einem beliebigen Standort in der Domäne abrufen, solange die Kopie den angegebenen Port verwendet. Für den Fall, dass eine der Kopien nicht verfügbar sein sollte, können mehrere Active-Directory-Kopien verwendet werden.
Port	Der Standardwert ist 636 (sicherer Port). SSL-Port des Verzeichnisservers; numerischer Wert.
Sicheren Port verwenden	Der Standardwert ist *Ein*. Gibt an, ob der Port sicher (Vorgabe) oder nicht sicher ist.

Verwandte Verfahrensweisen

Unterstützung für Verzeichnisdienst aktivieren

Verwandte Referenz

Optionen des Dialogfelds 'Server konfigurieren'

Dialogfeld 'Server konfigurieren' (Register 'Diagnose')

Tools ▸ Administration ▸ Server konfigurieren

Im Register **Diagnose** des Dialogfelds **Server konfigurieren** können Sie die Diagnostiktests für die Serverkonfiguration aktivieren.

Hinweis: Diese Optionen sind in der Regel aktiviert, wenn ein Mitarbeiter des Borland Technical Support ein Problem diagnostiziert.

Element	Beschreibung
Operationen zurückverfolgen mit einer Mindestdauer von ___ Millisekunden	Dieser Wert beträgt standardmäßig 0 Millisekunden. Erstellt eine .trc-Datei, mit der Befehle rückverfolgt werden können. Befehle werden rückverfolgt, wenn sie über eine Ausführungszeit verfügen, die der angegebenen Anzahl von Millisekunden entspricht oder diese überschreitet. Wenn der Wert 0 (Standard) verwendet wird, werden alle Befehle rückverfolgt.
Statistiküberwachung aktivieren. Aufzeichnen alle ___ Minuten	Ermöglicht die Aufzeichnung von Serverstatistiken, z. B. Speichernutzung, aktuell ausgeführte Befehle, Sperrstatistiken usw.
Unerwartete Zustände	Der Standardwert ist *Aus*. Erstellt eine Diagnosedatei (.dmp) für Asserts (Serverprotokolleinträge mit Codenummer 8).
Fehler	Der Standardwert ist *Aus*. Erstellt eine Diagnosedatei (.dmp) für Exceptions (Serverprotokolleinträge mit Codenummer 4).
Diagnosedateityp (Vorgabe ist 0)	Verwenden Sie diese Option nur auf Anweisung eines Mitarbeiters des technischen Supports von Borland. Wenn Sie auf **Jetzt generieren** klicken, wird eine Diagnosedatei (.dmp) erstellt. Sie wird im Protokollpfad der Serverkonfiguration gespeichert. Das Generieren der Datei kann einige Minuten dauern und während dieser Zeit werden keine anderen Serverprozesse ausgeführt.

Hinweis: Andere Diagnosedateitypen sollten unter der Anleitung der technischen Mitarbeiter von Borland angegeben und generiert werden.

Verwandte Verfahrensweisen

Serverprobleme diagnostizieren
Serverstatistik überwachen

Verwandte Referenz

Optionen des Dialogfelds 'Server konfigurieren'
Fehlerbehebung bei Problemen mit der Serverkonfiguration

Richtlinien für Datendateien und Transaktionsprotokolle

Dieser Abschnitt enthält Referenzinformationen hinsichtlich der Größe und Anzahl von Datendateien und Transaktionsprotokollen, die von einer mit einer Serverkonfiguration verknüpften Datenbank benötigt werden.

In diesem Abschnitt

Richtlinien für Microsoft SQL Server/SQL Server Express-Datendateien und -Transaktionsprotokolle

Die folgenden Empfehlungen von Borland gelten für Datendateien und Transaktionsprotokolle basierend auf der Anzahl der Benutzer. Die von Ihnen benötigten Größen können sich von den in der folgenden Tabelle angezeigten Werten unterscheiden.

Anzahl der Benutzer	Anzahl der Datendateien	Größe der jeweiligen Datendatei	Anzahl der Protokolldateien	Größe der jeweiligen Protokolldatei
Bis zu 15	3	50 MB	3	50 MB
Zwischen 15 und 50	3	300 MB	3	300 MB
Zwischen 51 und 100	5	300 MB	5	300 MB
Zwischen 101 und 300	7	500 MB	5	500 MB
> 300	7	800 MB	6	500 MB

Hinweis: Die Größe der Transaktionsprotokolldateien ist nur wichtig, wenn regelmäßig Sicherungskopien der Transaktionsprotokolle erstellt werden.

Das Erstellen von Sicherungskopien für Transaktionsprotokolle ist sehr wichtig. Wenn ein Backup einer Transaktion erstellt wurde, löschen Microsoft SQL Server- und SQL Server Expresss-Datenbanken automatisch den inaktiven Teil des Transaktionsprotokolls. Der inaktive Teil enthält abgeschlossene Transaktionen und wird daher bei einem Wiederherstellungsprozess nicht mehr benötigt. Der grundlegende Vorteil besteht darin, dass Microsoft SQL Server diesen inaktiven Platz des Transaktionsprotokolls wiederverwendet und so verhindert, dass das Transaktionsprotokoll immer größer wird und mehr Speicherplatz verbraucht. Hinsichtlich der Leistungssteigerung ist dies ein gewaltiges Plus.

Wenn Dateien automatisch größer werden, kann dies zu einer Fragmentierung führen, falls eine große Anzahl von Dateien auf derselben Festplatte gespeichert wird. Daher empfiehlt es sich, dass Dateien oder Dateigruppen auf so vielen verschiedenen lokalen Festplatten gespeichert werden, wie möglich. Platzieren Sie Objekte, die sehr viel Platz benötigen, in unterschiedlichen Dateigruppen.

Verwandte Verfahrensweisen

Mit Serverkonfigurationen arbeiten
Serverkonfigurationen erstellen

Richtlinien zu Datendateien für Oracle-Schema-Benutzer

Die folgenden Empfehlungen von Borland gelten für Datendateien basierend auf der Anzahl der Benutzer. Die von Ihnen benötigten Größen können sich von den in der folgenden Tabelle angezeigten Werten unterscheiden.

Anzahl der Benutzer	Anzahl der Datendateien	Größe der jeweiligen Datendatei
Bis zu 15	3	50 MB
Zwischen 15 und 50	3	300 MB
Zwischen 51 und 100	5	300 MB
Zwischen 101 und 300	7	500 MB
> 300	7	800 MB

Verwandte Verfahrensweisen

Mit Serverkonfigurationen arbeiten
Serverkonfigurationen erstellen

Referenzen für Initialisierungsdateien

Dieser Abschnitt enthält Referenzthemen, die sich mit Initialisierungsdateien befassen.

In diesem Abschnitt

Initialisierungsdateien suchen

Initialisierungsdateien werden bei den unterschiedlichen Windows-Plattformen an unterschiedlichen Speicherorten abgelegt. Unter NT lautet das Pfad-Präfix C:\ winnt\Profiles. Unter Windows 2000, XP und 2003 ist das Pfad-Präfix "C:\ Dokumente und Einstellungen".

- Die Datei "ClientLicenses.st" wird unter "\All Users\Anwendungsdaten\Borland\StarTeam\ClientLicenses.st" gespeichert. Sie wird von StarTeam-Runtime und den Anwendungs-Clients installiert. Wenn die Datei "ClientLicenses.st" fehlt, werden Sie aufgefordert, das Produkt zu registrieren.
- Die Datei "ConnectionManager.ini" (zum Starten der Anwendung) befindet sich unter "\All Users \Anwendungsdaten\Borland\StarTeam\ConnectionManager.ini". Sie wird von StarTeam-Runtime und den Anwendungs-Clients installiert. Wenn die Datei "ConnectionManager.ini" fehlt oder beschädigt ist, werden Sie gefragt, ob die Datei neu erstellt werden soll. Die fehlende ConnectionManager.ini-Datei kann auch durch eine erneute Installation neu erstellt werden.
- In der Datei "starteam-servers.xml" werden die Serverkonfigurationen aufgelistet, für die Sie Serverbeschreibungen angelegt haben (oder anlegen werden). Diese Beschreibungen werden zum Öffnen oder Erstellen von Projekten verwendet. Die Datei wird unter "\Benutzer\Anwendungsdaten\Borland\StarTeam \ServerList" gespeichert und wird von StarTeam-Runtime und den Anwendungs-Clients installiert.
- Die Server-Datei "starteam-server-configs.xml" enthält Serversitzungsinformationen und wird unter "Serverinstallationsordner\ starteam-server-configs.xml" gespeichert.
- Die Datei "starteam-client-options.xml" befindet sich unter "Pfad-Präfix\Benutzer\Anwendungsdaten\Borland \StarTeam\starteam-client-options.xml". Sie wird von StarTeam-Runtime und den Anwendungs-Clients installiert. In der starteam-client-options.xml-Datei werden die Einstellungen für Ihre persönlichen Optionen und ggf. in der Anwendung angelegte alternative Arbeitsordner gespeichert. Es wird empfohlen, eine Sicherungskopie dieser Datei anzulegen oder die Datei der Versionskontrolle zu unterstellen. Wenn die starteam-client-options.xml-Datei fehlt, wird sie automatisch von der Anwendung neu erstellt. In der neu erstellten Datei sind jedoch nur die Standardeinstellungen für die persönlichen Optionen und keine Informationen über alternative Arbeitsordner enthalten. Wenn die Datei "starteam-client-options.xml" beschädigt ist, kann sie gelöscht werden, aber möglicherweise können Sie sie auch bearbeiten. Es ist wahrscheinlich, dass die Datei "starteam-client-options.xml" fehlt oder beschädigt ist, wenn Ihre persönlichen Optionen nicht mehr korrekt sind, Änderungen, die Sie an persönlichen Optionen vorgenommen haben, nach einem Neustart der Anwendung nicht mehr vorhanden sind, Dateien sich nicht ändern, obwohl Sie sie ausgecheckt haben (da sie in die falschen Arbeitsordner kopiert wurden) oder die Anwendung meldet, dass alte Dateien fehlen und keine neuen Dateien gefunden werden, weil sie am falschen Ort danach sucht.

Verwandte Referenz

Referenzen für Initialisierungsdateien

ConnectionManager.ini

Die Datei "ConnectionManager.ini" enthält Informationen, die der Client für die Ausführung benötigt. Sie wird bei der Installation der Anwendung erstellt. Nachfolgend sehen Sie ein Beispiel für die ConnectionManager.ini-Datei. "x" sind Platzhalterzeichen für Hexadezimalzahlen.

```
[ConnectionManager]
WorkstationID=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

Verwandte Referenz

starteam-server-configs.xml
starteam-client-options.xml

starteam-server-configs.xml

Die Datei starteam-server-configs.xml enthält Sitzungsoptionen für eine oder mehrere Serverkonfigurationen. In den Serversitzungsoptionen werden die Hauptinformationen gespeichert, die der Server benötigt, um eine Serverkonfiguration zu starten. Für jeden Computer existiert eine "starteam-server-configs.xml"-Datei, die jeweils im gleichen Ordner wie die Server-Anwendung gespeichert wird. Unter Windows wird die Datei in der Regel unter C:\Programme\Borland\StarTeam Server gespeichert.

Die Sitzungsoptionsdaten jeder Serverkonfiguration beginnen mit dem Namen der Konfiguration in Klammern, gefolgt von Optionen und den zugehörigen Einstellungen. Der Server erstellt und verwaltet diese Datei, die beim Erstellen der ersten Serverkonfiguration erzeugt wird. Die Datei wird aktualisiert, wenn eine Serverkonfiguration erstellt, geändert, gelöscht, gestartet oder gestoppt wird. Bearbeiten Sie die Datei nicht direkt. Borland empfiehlt, eine Sicherungskopie der Datei starteam-server-configs.xml anzulegen oder die Datei der Versionskontrolle zu unterstellen.

Die Datei enthält folgende Informationen:

- CipherName: In Serverkonfigurationen, die mit Vorgängerversionen von StarTeam Server 5.3 erstellt wurden. Nur zur internen Verwendung. Bearbeiten Sie diese Option nicht.
- CipherSource: Nur zur internen Verwendung. Bearbeiten Sie diese Option nicht.
- CipherTest: Nur zur internen Verwendung. Bearbeiten Sie diese Option nicht.
- ComputerName: ComputerName identifiziert den Computer, auf dem sich der Server befindet. Die Option wird vom Server eingerichtet. Bearbeiten Sie diese Option nicht.
- CreatedByBuild: Gibt an, dass in der Serverkonfiguration keine Native-I-Archivdateien enthalten sein dürfen. Wird nur in Serverkonfigurationen verwendet, die mit StarTeam Server 2005 oder späteren Versionen erstellt werden.
- DBCreated: DBCreated gibt an, ob die von der Anwendung verwendeten Datenbanktabellen bereits erstellt wurden. Bearbeiten Sie diese Option nicht.
- DBServerName: Da auf alle Datenbanken mit ODBC zugegriffen wird, ist dies der Datenquellenname der Datenbank. In den Versionen 5.1 und 5.2 wurde auf Oracle-Datenbanken mit dem Oracle Net Service Name zugegriffen, der unter $ORACLE_HOME/network/admin/tnsnames.ora gespeichert ist. Dies trifft für StarTeam-Server unter Windows ab Version 5.3 nicht zu. Diese Information wird mit der Option -dsn des Befehls starteamserver angegeben. Sie können den Datenquellennamen prüfen, indem Sie die Optionen -view und -edit in der Befehlszeile angeben oder in der Anwendung im Dialogfeld das Register "Datenbank" anzeigen. Alle vorgenommenen Änderungen sind ab dem nächsten Start der Serverkonfiguration gültig.
- DBType: Verwenden Sie zum Angeben des Datenbanktyps einen der folgenden numerischen Werte. Diese Information wird mit der Option -t des Befehls starteamserver angegeben. Der Datenbanktyp kann nur beim Erstellen einer neuen Serverkonfiguration angegeben werden. Diese Informationen können für vorhandene Serverkonfigurationen nicht geändert werden. 2 = Microsoft SQL Server bzw. SSE oder 3 = Oracle. Sie können den Datenbanktyp prüfen, indem Sie in der Befehlszeile die Option -view angeben oder in der Anwendung das Register "Datenbank" des Dialogfelds "StarTeam-Serverkonfiguration" anzeigen.
- DBUserName und DBPassword: DBUserName und DBPassword entsprechen dem Namen und dem Passwort, mit denen die Anwendung auf die Serverkonfigurationsdatenbank zugreift. Diese Informationen werden mit den Optionen -u (für den Benutzernamen) und -p (für das Passwort) des Befehls starteamserver angegeben.
- DiagCommandTraceCutoffSize: Fügen Sie diese Option hinzu, um eine maximale Größe für Trace-Dateien festzulegen. Durch die Angabe <option name=”DiagCommandTraceCutoffSize” value=”5000000”/> wird die Größe der Trace-Datei beispielsweise auf 5000000 Byte begrenzt.
- Initialized: Initialized gibt an, ob die Serverkonfiguration initialisiert wurde. Die Option wird vom Server verwaltet. Bearbeiten Sie diese Option nicht.

- ItemCacheMemoryLimit: Legt fest, wie viel Arbeitsspeicher (in MB) für das Caching von Elementdaten maximal zur Verfügung steht. Der Standardwert ist -1, d. h., es gibt keine Begrenzung und der Server kann den für den Serverprozess maximal zur Verfügung stehenden Arbeitsspeicher für das Caching verwenden. Beispiel: Wenn Sie <option name="ItemCacheMemoryLimit" value="100"/> in der Konfigurationsdatei angeben, wird die Größe des Cache-Speichers auf 100 MB begrenzt.
- Die folgenden sechs Parameter definieren die relative Präferenz der Daten der jeweiligen Komponente im Serverdaten-Cache. DefaultValues = 0 für ItemCachePriority_Folder. DefaultValues = 100 für die restlichen Komponenten. Die einzelnen Komponenten belegen maximal ihren Prozent-"Anteil", der wie folgt berechnet wird (die Dateikomponente wird als Beispiel verwendet): FileShare% = (100 * ItemCachePriority_File) / (ItemCachePriority_File + ItemCachePriority_Change + ItemCachePriority_Requirement + ItemCachePriority_Task + ItemCachePriority_Topic + ItemCachePriority_Folder). DefaultValues = 100 für die restlichen Komponenten.
- ItemCachePriority_File
- ItemCachePriority_Change
- ItemCachePriority_Requirement
- ItemCachePriority_Task
- ItemCachePriority_Topic
- ItemCachePriority_Folder
- \ListenIP: Diese Option verbindet eine Serverkonfiguration mit einer bestimmten TCP/IP-Adresse (Sockets). Wenn der Server beispielsweise mehrere IP-Adressen (d. h. mehrere Netzwerkkarten) hat, können Sie den Server so konfigurieren, dass er einen bestimmten Port überwacht. Wenn diese Option auf 0 gesetzt wird (Standard), überwacht die Serverkonfiguration alle IP-Adressen des angegebenen Ports. Der Port, der auf dem Register **Protokoll** des Tools **Server konfigurieren** im Serveradministrations-Tool angegeben ist.
- LogPath: Gibt den Speicherort der Serverprotokolldatei an.
- MaxCommandThreads: Mit dieser Option wird die maximale Anzahl von Befehls-Threads angegeben, die die Serverkonfiguration erstellen kann. Der Standardwert für die maximale Anzahl von Befehls-Threads ist 16. Wenn Sie für diese Option den Wert 0 angeben, verwendet die Serverkonfiguration den Standardwert. MaxCommandThreads kann durch Bearbeiten der Datei starteam-server-configs.xml geändert werden. Diese Option sollte jedoch nur dann geändert werden, wenn dies durch einen StarTeam-Mitarbeiter empfohlen wird.
- MinCommandThreads: Mit dieser Option wird die minimale Anzahl von Befehls-Threads angegeben, die die Serverkonfiguration erstellt. Beim Start der Serverkonfiguration und während der Ausführung verfügt sie über mindestens so viele Befehls-Threads wie hier angegeben. Der Standardwert für die minimale Anzahl von Befehls-Threads ist 4. Wenn Sie für diese Option den Wert 0 angeben, verwendet die Serverkonfiguration den Standardwert. MinCommandThreads kann durch Bearbeiten der Datei starteam-server-configs.xml geändert werden. Diese Option sollte jedoch nur dann geändert werden, wenn dies durch einen StarTeam-Mitarbeiter empfohlen wird.
- PID: PID ist die *Prozess-ID* für die Instanz der Serverkonfiguration, die aktuell ausgeführt wird. Anderenfalls hat die Option den Wert 0. Die Option wird vom Server verwaltet. Bearbeiten Sie diese Option nicht. Wenn die Option fehlt, wird sie von starteamserver erstellt.
- RepositoryPath: RepositoryPath ist der vollständige Pfad des Repository-Ordners. Diese Information wird mit der Option -r des Befehls starteamserver angegeben. Der Repository-Pfad kann nur beim Erstellen einer neuen Serverkonfiguration angegeben werden. Diese Informationen können für vorhandene Serverkonfigurationen nicht geändert werden.
- Sample: Gibt die Beispielserverkonfiguration "StarDraw" von StarTeam an. Nur zur internen Verwendung. Bearbeiten Sie diese Option nicht.
- ServerGuid: Der Wert ServerGuid wird durch den Server bereitgestellt. Bearbeiten Sie diese Option nicht.

- UseAsyncIO: Microsoft empfiehlt die Verwendung von Async I/O für skalierbare Serveranwendungen, damit eine bessere Performance bei der Ausführung von Befehlen erzielt wird. Async I/O ist standardmäßig intern aktiviert. Beispiel: Wenn Sie <option name="UseAsyncIO" value="0"/> in der Konfigurationsdatei angeben, wird "Async I/O" deaktiviert.
- UserName: UserName ist der Domänenbenutzername des Benutzers, der die Serverkonfiguration erstellt hat. Die Option wird vom Server eingerichtet. Bearbeiten Sie diese Option nicht.
- ServiceMode: ServiceMode wird nur für Windows NT-Systeme benötigt. Geben Sie 1 an, um die Serverkonfiguration als NT-Dienst auszuführen. Geben Sie 0 an, um die Serverkonfiguration als Anwendung auszuführen.
- Status: Status gibt an, ob die Serverkonfiguration "Ready" (Bereit), "Starting" (Starten), "Running" (Wird ausgeführt) oder "Stopping" (Wird gestoppt) lautet Die Option wird vom Server verwaltet. Bearbeiten Sie diese Option nicht. Wenn die Option fehlt, wird sie von starteamserver erstellt.

Verwandte Referenz

ConnectionManager.ini
starteam-client-options.xml

starteam-client-options.xml

Die Datei "starteam-client-options.xml" enthält eine Zeile für jede Option, die im Dialogfeld "Persönliche Optionen" eingestellt werden kann. (Sie können das Dialogfeld öffnen, indem Sie im Menü **Tools** ▸ **Persönliche Optionen** wählen). Die meisten Optionsbezeichnungen in der Datei starteam-client-options.xml sind den englischen Bezeichnungen der entsprechenden Optionen in dem Dialogfeld sehr ähnlich. Für alle Optionen, die im Dialogfeld "Persönliche Optionen" über Auswahlfelder verfügen, wird der Wert 1 für "aktiviert" und der Wert 0 für "deaktiviert" vergeben. Je nach Option werden Intervalle auf eine Anzahl von Minuten oder Sekunden festgelegt. Pfade werden als Text angegeben. Im Text werden keine Anführungszeichen verwendet.

Beispielsweise enthält der Eintrag "Project Component" die Pfadangaben der alternativen Arbeitsordner für Projekte, auf die von Ihrer Workstation aus zugegriffen wird. Der Eintrag für diese Komponente in der starteam-client-options.xml-Datei besteht aus folgenden Teilen:

- Dem Text "Project Component".
- ViewWorkingFolderOverrides (Angabe eines alternativen Arbeitsordners für eine Ansicht) oder WorkingFolderOverrides (Angabe eines alternativen Arbeitsordners für einen einzelnen Ordner).
- Einer hexadezimalen Darstellung der Projektansicht und des Projektordners.
- Dem Pfad des alternativen Arbeitsordners.

Verwandte Referenz

starteam-server-configs.xml
ConnectionManager.ini

Referenzen für Serverprotokolldateien

Dieser Abschnitt enthält Referenzthemen, die sich mit Serverprotokolldateien befassen.

In diesem Abschnitt

Serverprotokoll

Die Serverprotokolldatei (Server.Länderkennung.Log) enthält die DBMS-Version und Build-Nummer. In der Datei werden zudem die Aktivitäten einer Serverkonfiguration aufgezeichnet. Bei jedem Start einer Serverkonfiguration benennt der Server die bestehende Protokolldatei um und erstellt eine neue Protokolldatei für die aktuelle Sitzung der Serverkonfiguration. Die Protokolldatei des vorhergehenden Starts der Konfiguration erhält einen Namen, der das Datum und die Uhrzeit des Zeitpunkts erhält, zu dem die Datei umbenannt wurde (Server.Länderkennung.Datum.Log). Wenn Sie beispielsweise eine Serverkonfiguration am 9. November 2005 um 17:22 Uhr starten, wird die alte Serverprotokolldatei in "Server.de-DE.2005-11-09-17-22-59.Log" umbenannt und es wird eine neue Serverprotokolldatei erstellt, deren Zeitstempel " 11/9/2005 17:23:03" lautet.

Wenn die Ländereinstellung des Betriebssystems, auf dem der Server ausgeführt wird, nicht "en-US" ist, werden zwei Serverprotokolldateien erstellt: eine für US-Englisch und eine für Ihre Ländereinstellung. Sie könnten beispielsweise die Dateien Server.en-US.Log und Server.de-De.Log haben. Das erste Protokoll wird für Unterstützungszwecke benötigt und das zweite kann von Ihnen verwendet werden.

Das Format setzt sich aus Zeilennummer, Code, Datums- und Zeitangabe und der Meldung zusammen. Die Codenummern haben keinerlei Bezug zum Schweregrad.

Serverprotokoll-Fehlercode

Das Format setzt sich aus Zeilennummer, Code, Datums- und Zeitangabe und der Meldung zusammen. Die Codenummern haben keinerlei Bezug zum Schweregrad.

```
Line #        Code          Date          Time          Error Message
-------------------------------------------------------------------------
45      00000001      2009-05-19      05:05:08          Message
46         00000002      2009-05-19      05:05:10          Warning
47         00000004      2009-05-19      05:05:12          Error
48         00000008      2009-05-19      05:05:14          Unexpected Condition
```

Verwandte Referenz

Referenzen für Serverprotokolldateien

Sicherheitsereignistypen

Wenn Sie über Zugriffsrechte für eine Serverkonfiguration verfügen, können Sie das entsprechende Sicherheitsereignisprotokoll jederzeit anzeigen. Das Sicherheitsereignisprotokoll ist keine gewöhnliche .Log-Datei, da die Daten des Protokolls in der Anwendungsdatenbank gespeichert werden. Diese Operation kann nur bei aktiviertem Server ausgeführt werden.

Ereignistyp	Beschreibung
Elementeigentümer hinzufügen	Gibt an, dass ein Benutzer einen Ordner oder ein Element erstellt hat.
Benutzer/Gruppe hinzufügen	Gibt an, dass der Serverkonfiguration ein Benutzer oder eine Gruppe hinzugefügt wurde.
Container-Zugriffsrechte hinzufügen/bearbeiten	Gibt an, dass die Zugriffsrechte für eine in einem anderen Objekt enthaltene Gruppe von Objekten hinzugefügt oder geändert wurden. Wenn Sie beispielsweise "Projekt > Zugriffsrechte" wählen und die Rechte für alle Änderungsanforderungen im Projekt ändern, passt dieses Ereignis in diese Kategorie.
Elementzugriffsrechte hinzufügen/bearbeiten	Gibt an, dass die Zugriffsrechte für ein bestimmtes Objekt hinzugefügt oder geändert wurden. Wenn Sie beispielsweise die Zugriffsrechte eines Projekts ändern, wird dieses Ereignis in dieser Kategorie aufgeführt.
Benutzer ändern	Gibt an, dass jemand Benutzernamen als Teil eines Replizierungsvorgangs geändert hat. Dieses Ereignis kann eintreten, wenn ein spezieller Client, z. B. Notification Agent, Operationen durchführt.
Container-Zugriffsrechte löschen	Gibt an, dass die Zugriffsrechte auf Container-Ebene gelöscht wurden.
Elementzugriffsrechte löschen	Gibt an, dass die Zugriffsrechte auf Elementebene gelöscht wurden.
Benutzer/Gruppe löschen	Gibt an, dass ein Benutzer oder eine Gruppe gelöscht wurde.
Benutzer/Gruppe bearbeiten	Gibt an, dass die Eigenschaften für einen Benutzer oder eine Gruppe geändert wurden.
Benutzerabmeldung erzwingen	Gibt an, dass ein Benutzer gezwungen wurde, sich von der Serverkonfiguration abzumelden.
Elementzugriffsprüfung	Gibt an, dass die Zugriffsrechte geprüft wurden, um zu sehen, ob der Benutzer auf ein bestimmtes Element zugreifen kann.
Abmeldung	Gibt an, dass ein Benutzer sich von der Serverkonfiguration abgemeldet hat.
Anmeldung	Gibt an, dass sich ein Benutzer bei der Serverkonfiguration angemeldet hat.
Anmeldeversuch: Konto gesperrt	Gibt an, dass ein Benutzer versucht hat, sich bei einem gesperrten Konto anzumelden.
Anmeldeversuch: Passwort abgelaufen	Gibt an, dass ein Benutzer versucht hat, sich mit einem abgelaufenen Passwort anzumelden.
Anmeldeversuch: Kein solcher Anmeldename	Gibt an, dass ein Benutzer versucht hat, sich mit einem nicht vorhandenen Benutzernamen anzumelden.
Anmeldeversuch: Eingeschränkte Zugriffszeit	Gibt an, dass ein Benutzer versucht hat, sich zu einer unzulässigen Zeit an einem Konto anzumelden.
Anmeldeversuch: Konto gesperrt	Gibt an, dass ein Benutzer versucht hat, sich mit einem deaktivierten Konto anzumelden.
Anmeldefehler	Gibt an, dass beim Anmeldeprozess ein falsches Passwort verwendet wurde.
Richtlinienänderung	Gibt an, dass eine Systemrichtlinie geändert wurde.

Benutzerstatusänderung	Gibt an, dass ein Administrator ein Benutzerkonto deaktiviert, reaktiviert, gesperrt, entsperrt oder eine Passwortänderung angefordert hat.

Verwandte Konzepte

Sicherheitsprotokolle

StarTeam.Log

In der StarTeam.Log-Datei werden alle Operationen protokolliert, die auf Ihrer Client-Workstation während einer Sitzung durchgeführt wurden. Die Datei dokumentiert Fehler und fehlgeschlagene Operationen zwischen dem Server und Ihrer Workstation während Serverkonfigurationssitzungen, sodass die Ursachen der Fehler leichter erkannt werden können. Die Datei enthält Befehle, die von Ihrer Workstation an eine Serverkonfiguration gesendet werden, wenn Sie ein Projekt öffnen und damit arbeiten, Befehle, die lokal auf Ihrer Workstation ausgeführt wurden, Fehlermeldungen, die bei Verwendung der Anwendung generiert wurden, oder Ereignisse, die von StarTeamMPX ausgeführt wurden. Jedes Mal, wenn Sie Ihren Client starten, erstellt das System eine StarTeam.Log-Datei in dem Ordner, den Sie in Ihren persönlichen Optionen angegeben haben. Auf den meisten Systemen befindet sich der Standard-Speicherort für die StarTeam.Log-Datei unter C:\Dokumente und Einstellungen\<Benutzername>\Anwendungsdaten\Borland\StarTeam. Wenn in dem Ordner bereits eine Datei namens "StarTeam.Log" vorhanden ist, benennt die Anwendung die vorhandene Datei um und fügt das Datum und die Uhrzeit der Umbenennung zum Dateinamen hinzu. Wenn Sie beispielsweise am 9. November 2005 um 10:35 Uhr eine StarTeam.Log-Datei erstellen, wird die alte StarTeam.Log -Datei in StarTeam-09-Nov-05-10-35-18.Log umbenannt und eine neue StarTeam.Log-Datei erstellt.

Da die Anwendung bei jedem Start des Clients eine neue StarTeam.Log-Datei erstellt, wächst die Größe des Ordners für die StarTeam-Protokolldatei möglicherweise sehr schnell an. Um die Anzahl der Protokolldateien in dem Ordner zu steuern, sollten Sie regelmäßig alte Protokolldateien aus dem Ausgabeordner löschen oder die StarTeam.Log-Option deaktivieren. Um diese Option zu deaktivieren, heben Sie die Markierungen der Auswahlfelder für Protokollfehler und Protokolloperationen im Register "Arbeitsbereich" des Dialogfelds "Persönliche Optionen" auf. Wählen Sie zum Anzeigen der StarTeam.Log-Datei in der Menüleiste **Tools** ▸ **StarTeam-Protokolldatei**. Sie können außerdem Daten aus einer StarTeam.Log-Datei in eine Anwendung importieren, die kommagetrennte Felder unterstützt, und in dieser anzeigen. Wenn Sie die Datei beispielsweise mit einer .csv-Erweiterung speichern, können Sie sie in Microsoft Excel öffnen.

Im Register "Arbeitsbereich" können Sie im Dialogfeld "Persönliche Optionen" den Speicherort der Datei "StarTeam.Log" und den Typ der im Protokoll aufzuzeichnenden Daten festlegen.

Verwandte Referenz

Referenzen für Serverprotokolldateien

DbConvert.<local>.log

In diesem Protokoll wird der Fortschritt der Datenbankmigration aufgezeichnet. "Migration" bezeichnet den Erstellungsprozess einer neuen Datenbank (Zieldatenbank) und das Kopieren von Daten aus einer vorhandenen Datenbank (Quelldatenbank) in die neue Datenbank.

Die Datei "DbConvert.log" besteht aus zwei Teilen (bei einer neuen Migration):

- Das Serverprotokoll für die neu erstellte Konfiguration mit einer Zieldatenbank. Dieses Serverprotokoll unterscheidet sich nicht vom Protokoll für das normale Starten oder Beenden eines Servers für eine neue Konfiguration.
- Das Migrationsprotokoll von der Migration der Quelldatenbank in die Zieldatenbank. Das Migrationsprotokoll beginnt nach der Zeile `***** Herunterfahren des Servers abgeschlossen *****` Es protokolliert den Quellkonfigurationsnamen und den Zielkonfigurationsnamen `Datenbankkonvertierung gestartet: Konvertierung der Konfiguration "Test" in die Konfiguration "TestMigrated"...` Beim Kopieren der Daten von der Quelldatenbank in die Zieldatenbank werden alle Tabellen aufgeführt: `"<Tabellenname> erfolgreich migriert"` Nach Abschluss des Kopiervorgang wird die Quellkonfiguration deaktiviert und die Zielkonfikuration wird aktiviert. `Quellkonfiguration erfolgreich deaktiviert` `Zielkonfiguration erfolgreich aktiviert` Zum Schluss steht die Meldung: `Migration erfolgreich abgeschlossen`.

Wenn die Migration angehalten und zu einem späteren Zeitpunkt neu gestartet wurde, ist das Serverprotokoll möglicherweise nicht in der Datei "DbConvert.log" enthalten, wenn die Zieldatenbank bereits bei einer vorherigen Ausführung der Migration erstellt wurde. Im Folgenden finden Sie ein Beispiel für dieses Protokoll:

```
1         00000001  2009-03-29 11:08:28  Microsoft Windows Server 2003-Familie Service Pack 2 (Build 3790)
2        00000001  2009-03-29 11:08:28  DSN: NewORA10R2_Hamachi, ODBC-Treiberversion: Oracle in OraDb10g_home1 10.02.0004
3        00000001  2009-03-29 11:08:29  Datenbankkonvertierung gestartet: Konvertierung der Konfiguration "newsql" in die Konfiguration "NewORA10R2_Hamachi"...
4         00000001  2009-03-29 11:08:30  Katalogtabellen erfolgreich konvertiert
5         00000001  2009-03-29 11:08:38  Katalogfelder erfolgreich konvertiert
6         00000001  2009-03-29 11:08:54  Katalogtabelle erfolgreich konvertiert
7         00000001  2009-03-29 11:08:54  Katalogtabelle erfolgreich konvertiert
8         00000001  2009-03-29 11:08:54  Katalogtabelle erfolgreich konvertiert
9         00000001  2009-03-29 11:08:56  Microsoft Windows Server 2003-Familie Service Pack 2 (Build 3790)
10       00000001  2009-03-29 11:08:56  DSN: NewORA10R2_Hamachi, ODBC-Treiberversion: Oracle in OraDb10g_home1 10.02.0004
11        00000001  2009-03-29 11:08:57  Server-Einstellungen erfolgreich migriert
12        00000001  2009-03-29 11:08:57  Kommunikationsprotokoll erfolgreich migriert
13        00000001  2009-03-29 11:08:57  IP-Bereichsobjekt erfolgreich migriert
14        00000001  2009-03-29 11:08:57  Benutzer erfolgreich migriert
15        00000001  2009-03-29 11:08:57  Gruppe erfolgreich migriert
16        00000001  2009-03-29 11:08:58  GroupMembers erfolgreich migriert
17        00000001  2009-03-29 11:08:58  AccessControlData erfolgreich migriert
18        00000001  2009-03-29 11:08:58  SystemPolicyObject2 erfolgreich migriert
19        00000001  2009-03-29 11:08:58  ObjectSecurityLog erfolgreich migriert
20        00000001  2009-03-29 11:08:58  Profiltyp erfolgreich migriert
21        00000001  2009-03-29 11:08:58  Profildaten erfolgreich migriert
22        00000001  2009-03-29 11:08:58  Zusammenführung erfolgreich migriert
23        00000001  2009-03-29 11:08:58  Projekt erfolgreich migriert
24        00000001  2009-03-29 11:08:58  Ansicht erfolgreich migriert
25        00000001  2009-03-29 11:08:58  Ordner erfolgreich migriert
26        00000001  2009-03-29 11:08:58  Ordner_QNodes erfolgreich migriert
27        00000001  2009-03-29 11:08:58  Ordner_QParts erfolgreich migriert
28        00000001  2009-03-29 11:08:58  Ordner_Queries2 erfolgreich migriert
```

```
29        00000001  2009-03-29 11:08:58  Ordner_Filters2 erfolgreich migriert
30        00000001  2009-03-29 11:08:59  Ordner_FColumns erfolgreich migriert
31        00000001  2009-03-29 11:08:59  ViewMember erfolgreich migriert
32        00000001  2009-03-29 11:08:59  ConfigLabel erfolgreich migriert
33        00000001  2009-03-29 11:08:59  ConfigLabelEntry erfolgreich migriert
34        00000001  2009-03-29 11:09:00  Link erfolgreich migriert
35        00000001  2009-03-29 11:09:00  LinkPin erfolgreich migriert
36        00000001  2009-03-29 11:09:01  PromotionDefinition erfolgreich migriert
37        00000001  2009-03-29 11:09:01  PromotionModel erfolgreich migriert
38        00000001  2009-03-29 11:09:01  PromotionState erfolgreich migriert
39        00000001  2009-03-29 11:09:01  PromotionStatus erfolgreich migriert
40        00000001  2009-03-29 11:09:01  ItemLock erfolgreich migriert
41        00000001  2009-03-29 11:09:01  Datei erfolgreich migriert
42        00000001  2009-03-29 11:09:01  Files_BookmarkObjects erfolgreich migriert
43        00000001  2009-03-29 11:09:01  Files_QNodes erfolgreich migriert
44        00000001  2009-03-29 11:09:01  Files_QParts erfolgreich migriert
45        00000001  2009-03-29 11:09:02  Files_Queries2 erfolgreich migriert
46        00000001  2009-03-29 11:09:02  Files_Filters2 erfolgreich migriert
47        00000001  2009-03-29 11:09:02  Files_FColumns erfolgreich migriert
48        00000001  2009-03-29 11:09:02  Änderung erfolgreich migriert
49        00000001  2009-03-29 11:09:02  Changes_UnreadObjects erfolgreich migriert
50        00000001  2009-03-29 11:09:02  Changes_BookmarkObjects erfolgreich migriert
51        00000001  2009-03-29 11:09:02  Changes_Attachments erfolgreich migriert
52        00000001  2009-03-29 11:09:03  Changes_QNodes erfolgreich migriert
53        00000001  2009-03-29 11:09:03  Changes_QParts erfolgreich migriert
54        00000001  2009-03-29 11:09:04  Changes_Queries2 erfolgreich migriert
55        00000001  2009-03-29 11:09:04  Changes_Filters2 erfolgreich migriert
56        00000001  2009-03-29 11:09:07  Changes_FColumns erfolgreich migriert
57        00000001  2009-03-29 11:09:07  Anforderung erfolgreich migriert
58        00000001  2009-03-29 11:09:07  Requirements_Attachments erfolgreich migriert
59        00000001  2009-03-29 11:09:07  Requirements_UnreadObjects erfolgreich migriert
60        00000001  2009-03-29 11:09:07  Requiremen_BookmarkObjects erfolgreich migriert
61        00000001  2009-03-29 11:09:07  Requirements_QNodes erfolgreich migriert
62        00000001  2009-03-29 11:09:07  Requirements_QParts erfolgreich migriert
63        00000001  2009-03-29 11:09:07  Requirements_Queries2 erfolgreich migriert
64        00000001  2009-03-29 11:09:08  Requirements_Filters2 erfolgreich migriert
65        00000001  2009-03-29 11:09:08  Requirements_FColumns erfolgreich migriert
66        00000001  2009-03-29 11:09:08  Task erfolgreich migriert
67        00000001  2009-03-29 11:09:08  WorkRecord erfolgreich migriert
68        00000001  2009-03-29 11:09:08  Abhängigkeiten erfolgreich migriert
69        00000001  2009-03-29 11:09:08  Tasks_UnreadObjects erfolgreich migriert
70        00000001  2009-03-29 11:09:08  Tasks_BookmarkObjects erfolgreich migriert
71        00000001  2009-03-29 11:09:08  Tasks_Attachments erfolgreich migriert
72        00000001  2009-03-29 11:09:09  Tasks_QNodes erfolgreich migriert
73        00000001  2009-03-29 11:09:09  Tasks_QParts erfolgreich migriert
74        00000001  2009-03-29 11:09:09  Tasks_Queries2 erfolgreich migriert
75        00000001  2009-03-29 11:09:09  Tasks_Filters2 erfolgreich migriert
76        00000001  2009-03-29 11:09:09  Tasks_FColumns erfolgreich migriert
77        00000001  2009-03-29 11:09:10  Thema erfolgreich migriert
78        00000001  2009-03-29 11:09:10  Topics_Attachments erfolgreich migriert
79        00000001  2009-03-29 11:09:10  Topics_UnreadObjects erfolgreich migriert
80        00000001  2009-03-29 11:09:10  Topics_BookmarkObjects erfolgreich migriert
81        00000001  2009-03-29 11:09:10  Topics_QNodes erfolgreich migriert
82        00000001  2009-03-29 11:09:10  Topics_QParts erfolgreich migriert
83        00000001  2009-03-29 11:09:10  Topics_Queries2 erfolgreich migriert
84        00000001  2009-03-29 11:09:10  Topics_Filters2 erfolgreich migriert
85        00000001  2009-03-29 11:09:11  Topics_FColumns erfolgreich migriert
86        00000001  2009-03-29 11:09:12  Trace erfolgreich migriert
87        00000001  2009-03-29 11:09:12  Traces_LinkValues erfolgreich migriert
88        00000001  2009-03-29 11:09:12  Traces_UnreadObjects erfolgreich migriert
89        00000001  2009-03-29 11:09:12  Traces_BookmarkObjects erfolgreich migriert
```

```
90        00000001  2009-03-29 11:09:12  Traces_Attachments erfolgreich migriert
91        00000001  2009-03-29 11:09:12  Traces_QNodes erfolgreich migriert
92        00000001  2009-03-29 11:09:12  Traces_QParts erfolgreich migriert
93        00000001  2009-03-29 11:09:12  Traces_Queries2 erfolgreich migriert
94        00000001  2009-03-29 11:09:12  Traces_Filters2 erfolgreich migriert
95        00000001  2009-03-29 11:09:12  Traces_FColumns erfolgreich migriert
96        00000001  2009-03-29 11:09:13  Audits erfolgreich migriert
97        00000001  2009-03-29 11:09:13  Audits_QNodes erfolgreich migriert
98        00000001  2009-03-29 11:09:13  Audits_QParts erfolgreich migriert
99        00000001  2009-03-29 11:09:13  Audits_Queries2 erfolgreich migriert
100       00000001  2009-03-29 11:09:13  Audits_Filters2 erfolgreich migriert
101       00000001  2009-03-29 11:09:13  Audits_FColumns erfolgreich migriert
102       00000001  2009-03-29 11:09:14  ChangePackage erfolgreich migriert
103       00000001  2009-03-29 11:09:14  ChangePackageChange erfolgreich migriert
104       00000001  2009-03-29 11:09:14  ChangeReference erfolgreich migriert
105       00000001  2009-03-29 11:09:14  ChangePackag_UnreadObjects erfolgreich migriert
106       00000001  2009-03-29 11:09:14  ChangePack_BookmarkObjects erfolgreich migriert
107       00000001  2009-03-29 11:09:14  ChangePackages_Attachments erfolgreich migriert
108       00000001  2009-03-29 11:09:14  ChangePackages_QNodes erfolgreich migriert
109       00000001  2009-03-29 11:09:14  ChangePackages_QParts erfolgreich migriert
110       00000001  2009-03-29 11:09:14  ChangePackages_Queries2 erfolgreich migriert
111       00000001  2009-03-29 11:09:14  ChangePackages_Filters2 erfolgreich migriert
112       00000001  2009-03-29 11:09:15  ChangePackages_FColumns erfolgreich migriert
113       00000001  2009-03-29 11:09:15  Workstation erfolgreich migriert
114       00000001  2009-03-29 11:09:15  Quellkonfiguration erfolgreich deaktiviert
115       00000001  2009-03-29 11:09:15  Zielkonfiguration erfolgreich aktiviert
116       00000001  2009-03-29 11:09:15  Migration erfolgreich abgeschlossen.
```

Verwandte Referenz

Referenzen für Serverprotokolldateien

Symbole für den Serverkonfigurationsstatus

Wenn Sie das Serveradministrations-Tool verwenden, werden links neben den Serverkonfigurationen Symbole angezeigt, die den Status der Konfigurationen angeben. Diese Symbole werden im Folgenden beschrieben.

Symbol	Beschreibung
	Eine laufende Serverkonfiguration.
	Eine Serverkonfiguration, die gestartet wird.
	Eine Serverkonfiguration, die als Windows-Dienst ausgeführt wird.
	Eine Serverkonfiguration, die nicht ausgeführt wird.
	Eine neue Serverkonfiguration, die nicht ausgeführt wird, aber aktiviert ist.
	Eine aktivierte Serverkonfiguration, die nicht ausgeführt wird, aber zum Ausführen als Windows-Dienst eingerichtet ist.
	Eine deaktivierte Serverkonfiguration.
	Eine Serverkonfiguration, die heruntergefahren wird.

Verwandte Verfahrensweisen

Mit Serverkonfigurationen arbeiten

Fehlerbehebung bei Problemen mit der Serverkonfiguration

Um die Zeit zu verringern, die für die Diagnose von Problemen benötigt wird, stellt das Programm Tracing- und Debugging-Tools für den Server zur Verfügung. Mit diesen Tools können Trace-Befehlsdateien und/oder Diagnosedateien (.dmp) erstellt werden.

Befehle verfolgen	Mit der Trace-Option wird eine Datei erstellt, in der einzelne Serverbefehle aufgezeichnet werden. Zu verfolgende Befehle müssen über eine Ausführungszeit verfügen, die der angegebenen Anzahl Millisekunden entspricht oder diese überschreitet. Die vorgegebene Zeit ist 0. Wenn Sie nur Befehle mit einer längeren Ausführungszeit aufzeichnen möchten, müssen Sie diese Einstellung anpassen, um ein unnötiges Anwachsen der Trace-Datei zu vermeiden. Trace-Dateien sollten nicht mehr als 10 MB Daten pro Tag erzeugen. In der Regel sehen Benutzer nur einen kleinen Teil dieser pro Tag erzeugten Daten. Trace-Daten werden in der Datei `Server.trc` gespeichert, die sich aus einem Header und einer beliebigen Anzahl von Datensätzen zusammensetzt. Wenn ein Trace endet, weist der Server der vorhandenen Datei den Zeitstempel `Server.Zeit.trc` zu. Trace-Dateien werden unter `Repository-Pfad\Log\Trace` gespeichert. Die nächste Trace-Datei wird erzeugt, wenn die Serverkonfiguration neu gestartet oder die Trace-Option aktiviert wird.
Diagnosedateien (.dmp)	Das Programm erzeugt einige Minidump-Dateien automatisch, während andere nur erstellt werden, wenn die .dmp-Optionen aktiviert sind. Minidump-Dateien können für eines oder beide der folgenden Ereignisse erstellt werden: ■ Asserts (unerwartete Bedingungen). Serverprotokolleinträge mit der Codenummer 8. ■ Exceptions (Fehler, in der Regel Zugriffsverletzungen). Serverprotokolleinträge mit der Codenummer 4. Minidump-Dateien werden am selben Speicherort erstellt wie die Serverprotokolldatei. Die allgemeine Namenskonvention für diese Dateien lautet `Präfix-Zähler-Zeit.dmp`, wobei "Präfix" die Quelle des Dumps angibt, "Zähler" eine Ganzzahl ist, die bei jeder folgenden .dmp-Datei erhöht wird, damit die Namen garantiert eindeutig sind, und "Zeit" für die lokale Serverzeit steht, zu der der Dump erzeugt wurde.

Verwandte Verfahrensweisen

Serverprobleme diagnostizieren

Verwandte Referenz

Dialogfeld 'Server konfigurieren' (Register 'Diagnose')
Serverprotokoll

Zugriffsrechte und Berechtigungen

Dieser Abschnitt enthält Referenzthemen, die sich mit Zugriffsrechten und Berechtigungen befassen.

In diesem Abschnitt

Gruppenberechtigungen
Beschreibt die einer Gruppe zugewiesenen Berechtigungen.

Serverzugriffsrechte
Beschreibt Zugriffsrechte auf Serverebene.

Projekt - Zugriffsrechte
Beschreibt allgemeine Zugriffsrechte für Projekte.

Ansicht - Zugriffsrechte
Beschreibt die Zugriffsrechte für Ansichten.

Zugriffsrechte für Ordner
Beschreibt die Zugriffsrechte für Ordner.

Zugriffsrechte für untergeordnete Ordner
Beschreibt die Zugriffsrechte für untergeordnete Ordner.

Datei - Zugriffsrechte
Beschreibt Zugriffsrechte für Dateien.

Allgemeine Elementzugriffsrechte ändern
Beschreibt allgemeine Elementzugriffsrechte, die über den Knoten "Datei" in den Dialogfeldern "Projekt - Zugriffsrechte", "Ansicht - Zugriffsrechte", "Ordner - Zugriffsrechte" und "Datei - Zugriffsrechte" verfügbar sind.

Zugriffsrechte für Heraufstufungsstatuswerte
Beschreibt die Zugriffsrechte für Heraufstufungsstatuswerte.

Komponentenzugriffsrechte
Beschreibt die Zugriffsrechte für Komponenten.

Filterzugriffsrechte auf Komponentenebene
Beschreibt die Zugriffsrechte für Filter auf Komponentenebene.

Zugriffsrechte für einzelne Filter
Beschreibt die Zugriffsrechte für einzelne Filter.

Abfragezugriffsrechte auf Komponentenebene
Beschreibt die Zugriffsrechte für Abfragen auf Komponentenebene.

Zugriffsrechte für einzelne Abfrage
Beschreibt die Zugriffsrechte für einzelne Abfragen.

Gruppenberechtigungen

Durch die einer Gruppe zugewiesenen Berechtigungen erhalten Mitglieder der Gruppe möglicherweise das Recht, auf Objekte zuzugreifen und Operationen auszuführen, für die sie normalerweise keine Rechte haben. Mit anderen Worten: Berechtigungen haben Vorrang vor Einstellungen für Zugriffsrechte.

Wenn Sie im Dialogfeld "Serveradministration" auf "Benutzer-Manager" klicken, werden Sie feststellen, dass die Serverkonfiguration über einige Standardgruppen verfügt: "All Users", "Administrators", "System Managers" und "Security Administrators". Der Standardbenutzer mit dem Namen "Administrator" ist Mitglied der Gruppen "Administrators" und "Security Administrators". Standardmäßig verfügt die Administratorengruppe über alle Gruppenberechtigungen. Alle anderen Gruppen verfügen standardmäßig über keine dieser Berechtigungen.

Alle Mitglieder einer Gruppe haben für jedes von der Serverkonfiguration verwaltete Projekt dieselben Berechtigungen. Die Berechtigungen gelten in gleichem Maß für alle Ebenen: Projekte, Ansichten, Ordner und Elemente in Ordnern. Wenn Benutzer mehreren Gruppen angehören, verfügen sie über die maximale Anzahl an Berechtigungen, unabhängig davon, welche Gruppe diese Berechtigungen gewährt.

Diese Berechtigung...	ermöglicht einer Gruppe Folgendes auszuführen...
Objekt und seine Eigenschaften anzeigen	Berechtigt zum Anzeigen von Projekten, Ansichten, Ordnern, Elementen und ihren Eigenschaften. Diese Berechtigung hat Vorrang vor dem ähnlichen Zugriffsrecht, das im Dialogfeld Zugriffsrechte unter "Allgemeine Rechte für Objekt" festgelegt werden kann.
Objekteigenschaften ändern	Berechtigt zum Ändern von Eigenschaften von Projekten, Ansichten, Ordnern oder Elementen. Diese Berechtigung hat Vorrang vor dem ähnlichen Zugriffsrecht, das im Dialogfeld Zugriffsrechte unter "Allgemeine Rechte für Objekt" festgelegt werden kann.
Objekt löschen	Berechtigt zum Löschen von Projekten, Ansichten, Ordnern oder Elementen. Diese Berechtigung hat Vorrang vor dem ähnlichen Zugriffsrecht, das im Dialogfeld Zugriffsrechte unter "Allgemeine Rechte für Objekt" festgelegt werden kann.
Objekt entfernen (dauerhaft löschen)	Diese Berechtigung wird derzeit nicht unterstützt.
Einstellungen für die Objektsicherheit ändern	Berechtigt zum Ändern von Zugriffsrechten für Projekte, Ansichten, Ordner oder Elemente. Diese Berechtigung hat Vorrang vor dem ähnlichen Zugriffsrecht, das im Dialogfeld Zugriffsrechte unter "Allgemeine Rechte für Objekt" festgelegt werden kann.
Objekt erstellen und in einem Container ablegen	Berechtigt zum Erstellen neuer Objekte und Ablegen derselben in Containern. Gleichzeitig kann diese Gruppe neue Ansichten zu einem Projekt, neue Ordner zu einer Ansicht und neue Ordner und Elemente zu einem Ordner hinzufügen. Diese Berechtigung hat Vorrang vor dem ähnlichen Zugriffsrecht, das im Dialogfeld Zugriffsrechte unter "Allgemeine Rechte für Objekt" festgelegt werden kann. Sie hat keinen Vorrang vor dem Zugriffsrecht auf Serverebene, das Benutzern das Erstellen von Projekten ermöglicht.
Sämtliche Zugriffsrechte auf Klassenebene für alle Objektklassen gewähren	Berechtigt zum Ausführen von Operationen, die von den vorhergehenden Berechtigungen nicht abgedeckt werden. Diese Berechtigung ermöglicht Gruppenmitgliedern beispielsweise das Auschecken von Dateien, das Umgehen von Sperren und das Ausführen von Verknüpfungs- und Labeling-Vorgängen. Diese Berechtigung hat Vorrang vor

	einigen der Zugriffsrechte, die im Dialogfeld "Zugriffsrechte" unter "Allgemeine Rechte für Objekt-Container" gewährt werden können, sowie vor allen <Element>-spezifischen Zugriffsrechten.

Verwandte Referenz

Zugriffsrechte und Berechtigungen

Serverzugriffsrechte

Durch die Zugriffsrechte auf Serverebene werden Benutzer und Gruppen autorisiert, Operationen in einer bestimmten Serverkonfiguration auszuführen. Eine der Optionen legt fest, wer Projekte erstellen darf, wenn die Serverkonfiguration ausgeführt wird, und wer nicht. Serverzugriffsrechte können nur bei aktiviertem Server zugewiesen werden.

Standardmäßig werden der Gruppe "Administrators" alle Projekt- und Serverrechte zugewiesen. Die Gruppe "All Users" verfügt standardmäßig über die Rechte zum Erstellen von Projekten und zum Anzeigen der Serverkonfiguration und des Serverprotokolls. Die Serverzugriffsrechte werden in der folgenden Tabelle zusammengefasst.

Dieses Zugriffsrecht...	Ermöglicht einem Benutzer oder einer Gruppe Folgendes auszuführen...
Serverprotokoll anzeigen	Überprüfen Sie die Serverprotokollinformationen. Diese können nicht geändert werden.
Statistiken und Lizenzinformationen anzeigen	Das Überprüfen der statistischen Informationen (StarTeam Server 5.4 und älter). Das Ändern ist nicht möglich. Das Erstellen von Lizenznutzungsdateien.
Serverkonfiguration anzeigen	Überprüfen Sie die Serverkonfigurationsoptionen. Diese können nicht geändert werden.
Serverkonfiguration ändern	Ändern der Serverkonfigurationsoptionen.
Server remote verwalten	Das Sperren bzw. Freigeben von Servern, das Starten und Herunterfahren von Servern über den Client, das Zugreifen auf die Schalter zum Starten/Stoppen der Konvertierung und das Zugreifen auf die Schalter für den Hive-Manager-Datenspeicher.
Benutzerkonten verwalten	Fügen Sie Benutzer und Gruppen hinzu.
Systemrichtlinie anzeigen	Überprüfen der Optionen für Passwörter und Anmeldefehler. Das Ändern ist nicht möglich.
Systemrichtlinie ändern	Das Ändern von Optionen für Passwörter und Anmeldefehler für die Serverkonfiguration.
Einstellungen für die Serversicherheit ändern	Legen Sie die Serverzugriffsrechte fest. Stellen Sie sicher, dass Sie auch weiterhin zu den Benutzern gehören, die Zugriffsrechte ändern können, wenn Sie diese Einstellung ändern.
Sicherheitsprotokoll anzeigen	Das Überprüfen der Serverprotokollinformationen. Das Ändern ist nicht möglich.
StarDisk-Operationen	
Neue Benutzer erstellen	Das Hinzufügen neuer Benutzer zum Beispielprojekt.
Replizierungsunterstützung	
Benutzer/Verarbeitungszeit ändern	Das Ändern der Erstellungszeiten und Benutzernamen, wenn spezielle Clients verwendet werden, wie beispielsweise der Notification Agent.
Projektbezogene Operationen	
Projekte erstellen	Das Erstellen von Projekten, wenn der Server mit dieser Serverkonfiguration läuft.
Anpassungen	
Datenbankschema hinzufügen/ändern	Das Erstellen von benutzerdefinierten Feldern als Elementeigenschaften oder das Ändern von anpassbaren Feldern eines Elements.
Komponentenbasierte Operationen	
Zugriffsrechte für Komponenten verwalten	Mit diesen Rechten werden die Benutzer und Gruppen festgelegt, die für bestimmte Komponenten der Serverkonfiguration Filter und Abfragen erstellen und anwenden können.

Verwandte Referenz

Zugriffsrechte und Berechtigungen

Projekt - Zugriffsrechte

In der folgenden Tabelle werden die allgemeinen Objektrechte für ein Projekt beschrieben. Wählen Sie **Projekt ▸ Zugriffsrechte**, um das Dialogfeld "Projekt - Zugriffsrechte" anzuzeigen. Das Recht zum Erstellen eines Projekts wird als Server-Zugriffsrecht festgelegt.

Dieses Zugriffsrecht	Ermöglicht einem Benutzer oder einer Gruppe Folgendes auszuführen...
Objekt und seine Eigenschaften anzeigen	Anzeigen des Projekts und der Eigenschaften durch Wählen von "Projekt > Eigenschaften".
Eigenschaften ändern	Ändern Sie die Eigenschaften des Projekts. Folgende Projekteigenschaften können geändert werden: Name, Beschreibung, Schlüsselworterweiterungseinstellungen, Einstellungen für alternative Eigenschaftseditoren (APEs), Einstellungen für Prozessregeln, Erzwingen des Schreibschutzes für nicht gesperrte Dateien und einige Einstellungen, die Benutzer betreffen (z. B. die erforderliche Eingabe von Revisionskommentaren beim Einchecken von Dateien).
Objekt löschen	Löschen Sie das Projekt aus seiner Serverkonfiguration.
Objektzugriffsrechte ändern	Ändern Sie die Zugriffsrechte für dieses Projekt. Stellen Sie sicher, dass Sie auch weiterhin zu den Benutzern gehören, die Zugriffsrechte ändern können, wenn Sie diese Einstellung ändern.

Verwandte Referenz

Zugriffsrechte und Berechtigungen

Ansicht - Zugriffsrechte

Wenn Sie **Ansicht ▸ Zugriffrechte** wählen, um das Dialogfeld **Ansicht - Zugriffsrechte** zu öffnen, werden die Rechte für die aktuelle Ansicht angezeigt. Die für die **Ansicht** verfügbaren Rechte sind auch über den Knoten **Ansicht** im Dialogfeld **Projekt - Zugriffsrechte** verfügbar. Im letzteren Dialogfeld betreffen die Rechte alle Ansichten des Projekts statt einer bestimmten Ansicht. Es beinhaltet außerdem ein Recht auf Containerebene, mit dem Benutzer oder Gruppen Ansichten für das Projekt erstellen können. Dieses Recht ist im Knoten **Ansicht** des Dialogfelds **Ansicht - Zugriffsrechte** verfügbar.

In der folgenden Tabelle werden die über den Knoten **Ansicht** im Dialogfeld **Projekt - Zugriffsrechte** verfügbaren Zugriffsrechte beschrieben. Die meisten dieser Zugriffsrechte werden auch im Knoten **Ansicht** des Dialogfelds **Ansicht - Zugriffsrechte** angezeigt, gelten dann aber nur für die aktuelle Ansicht.

Dieses Zugriffsrecht...	Ermöglicht einem Benutzer oder einer Gruppe Folgendes auszuführen...
Allgemeine Rechte für Objekt	
Objekt und seine Eigenschaften anzeigen	Ändern der Ansichtseigenschaften. Die Eigenschaften, die für eine Ansicht geändert werden können, sind der Name der Ansicht, die Beschreibung, der Arbeitsordner (der auch der Arbeitsordner des Stammordners ist), die Verzweigungseinstellung für gemeinsam genutzte Elemente und die Einstellung für das Dateistatus-Repository.
Eigenschaften ändern	Ändert die Ansichtseigenschaften.
Objekt löschen	Löscht das Objekt aus der Ansicht.
Objektzugriffsrechte ändern	Ändert die Zugriffsrechte des ausgewählten Objekts in der Ansicht.
Ansichtsspezifische Rechte	
Ansichts-Labels erstellen	Erstellt Ansichts-Labels. Diese Ansichts-Labels werden den Ordnern und Elementen der Ansicht automatisch zugewiesen. Benutzer, die nur über das Recht zum Erstellen, nicht aber zum Zuweisen von Labels verfügen, können trotzdem Labels erstellen.
Ansichts-Labels ändern	Ändert die Eigenschaften von Ansichts-Labels. Durch dieses Recht können Benutzer beispielsweise Labels einfrieren, damit diese nicht mehr angepasst werden können.
Ansichts-Labels löschen	Löscht Ansichts-Labels. Gelöschte Ansichts-Labels werden automatisch von Ordnern und Elementen gelöst, denen Sie zuvor zugewiesen waren. Benutzer, die nur über das Recht zum Löschen von Ansichts-Labels verfügen, nicht aber zum Lösen derselben, können dennoch Ansichts-Labels löschen.
Revisions-Labels erstellen	Erstellt Revisions-Labels. Benutzer, die nur über das Recht zum Erstellen, nicht aber zum Zuweisen von Labels verfügen, können trotzdem Labels erstellen.
Revisions-Labels ändern	Ändert die Eigenschaften von Revisions-Labels. Durch dieses Recht können Benutzer beispielsweise Labels einfrieren, damit diese nicht mehr angepasst werden können.
Revisions-Labels löschen	Löscht Revisions-Labels. Gelöschte Labels werden automatisch von Ordnern und Elementen gelöst, denen Sie zuvor zugewiesen waren. Benutzer, die nur über das Recht zum Löschen, nicht aber zum Lösen von Revisions-Labels verfügen, können trotzdem Revisions-Labels löschen.
Heraufstufungsmodell festlegen	Erstellt, löscht und ändert die Reihenfolge von Heraufstufungsstatuswerten und ermöglicht das Bearbeiten deren Eigenschaften. Nachdem Sie einen neuen Heraufstufungsstatus erstellt haben, müssen Sie das Dialogfeld "Heraufstufung" verlassen und erneut öffnen, um Zugriffsrechte für den neuen Status festlegen zu können.

Ansichten erstellen	Erstellt Ansichten im aktuellen Projekt. Dieses Recht auf Containerebene steht Ihnen nur zur Verfügung, wenn Sie im Dialogfeld "Projekt - Zugriffsrechte" den Knoten "Ansicht" wählen.
Standardtypen überschreiben	Ermöglicht Benutzern, die beim Erstellen einer neuen Ansicht vorgegebenen Ansichtstypen zu überschreiben.

Verwandte Referenz

Zugriffsrechte und Berechtigungen

Zugriffsrechte für Ordner

Wenn Sie **Ordner** ▸ **Erweitert** ▸ **Zugriffsrechte** wählen, um das Dialogfeld "Ordner - Zugriffsrechte" zu öffnen, werden zwei Ordnerknoten angezeigt. Die unter "Dieser Ordner" verfügbaren Rechte gelten nur für den ausgewählten Ordner. Die unter "Untergeordnete Ordner" verfügbaren Rechte gelten für alle Unterordner des ausgewählten Ordners. Das im Folgenden gezeigte Dialogfeld und die nachfolgende Tabelle beziehen sich auf den aktuellen Ordner. In der Tabelle werden die unter "Dieser Ordner" im Dialogfeld "Ordner - Zugriffsrechte" verfügbaren Zugriffsrechte beschrieben.

Hinweis: Da "Dieser Ordner" über keine Unterkategorie für allgemeine Element-Containerrechte verfügt, werden Containerrechte für "Diesen Ordner" mithilfe des Knotens "Untergeordnete Ordner" des übergeordneten Ordners festgelegt. Wenn "Dieser Ordner" der Stammordner ist, werden diese Rechte im Knoten "Untergeordnete Ordner" des Dialogfelds "Ansicht - Zugriffsrechte" festgelegt.

Dieses Zugriffsrecht...	Ermöglicht einem Benutzer oder einer Gruppe Folgendes auszuführen...
Allgemeine Rechte für Objekt	
Element und seine Eigenschaften anzeigen	Anzeigen der Register "Name", "Ausschließen" und "Dateien" durch Auswahl von "Ordner > Eigenschaften". Die Anzeige des Registers "Historie" wird durch das Ordnerzugriffsrecht "Historie anzeigen" gesteuert. Die Anzeige des Registers "Link" in StarTeam wird durch das Ordnerzugriffsrecht "Links anzeigen" gesteuert.
Eigenschaften ändern	Ändern der Ordnereigenschaften in den Registern "Name" und "Ausschließen" des Ordners. Zu den Eigenschaften gehören der Ordnername, die Beschreibung, die Verwendung von geerbten und lokalen Ausschlusslisten und der Inhalt der lokalen Ausschlussliste. Wenn der Ordner kein Stammordner ist, gehören der Arbeitsordner und die Einstellungen für den alternativen Arbeitsordner ebenfalls zu den Ordnereigenschaften. Bei Stammordnern gehören die Arbeitsordner zu den Ansichtseigenschaften und werden durch dieses Zugriffsrecht nicht gesteuert.
Aus Ordner löschen	Löschen des Ordners aus seinem übergeordneten Ordner. Beachten Sie, dass Sie einen Ordner auch löschen können, wenn Sie über das Recht verfügen, einen der übergeordneten Ordner dieses Ordners zu löschen.
Elementzugriffsrechte ändern	Ändern Sie die Zugriffsrechte für den Ordner. Stellen Sie sicher, dass Sie auch weiterhin zu den Benutzern gehören, die Zugriffsrechte ändern können, wenn Sie diese Einstellung ändern.
Historie anzeigen	Anzeigen des Registers "Historie" des Ordners durch Auswählen von **Ordner** ▸ **Eigenschaften**.
Wartung durchführen	Ändern der Revisionskommentare für zurückliegende Revisionen.
Exklusive Sperren einstellen	Sperren Sie Ordner exklusiv.
Exklusive Sperren außer Kraft setzen	Entfernen Sie die exklusive Sperre eines anderen Benutzers für die Ordner.
Label-Rechte	
Ansichts-Labels anhängen/anpassen	Fügen Sie ein Ansichts-Label für diesen Ordner hinzu. Verschieben Sie ein Ansichts-Label von einer Revision eines Ordners zu einer anderen. Durch dieses Recht wird die direkte Änderung von Labels dieses Ordners auf Ordnerebene gesteuert. Benutzer können dem Ordner weiterhin neu erstellte Ansichts-Labels zuweisen.
Ansichts-Labels lösen	Entfernen Sie ein Ansichts-Label dieses Ordners. Beachten Sie, dass Benutzer, die Ansichts-Labels löschen können, auch Ansichts-Labels von diesem Ordner lösen können, indem sie das Label aus der Ansicht löschen und somit die Einstellung dieses Zugriffsrechts umgehen.

Revisions-Labels anhängen/anpassen	Fügen Sie ein Revisions-Label für diesen Ordner hinzu. Verschieben Sie ein Revisions-Label von einer Revision eines Ordners zu einer anderen. Durch dieses Recht wird die direkte Änderung von Revisions-Labels dieses Ordners auf Ordnerebene gesteuert.
Revisions-Labels lösen	Entfernen Sie ein Revisions-Label dieses Ordners. Beachten Sie, dass Benutzer, die Revisions-Labels löschen können, auch Revisions-Labels von dem Ordner lösen können, indem sie das Label aus der Ansicht löschen und somit die Einstellung dieses Zugriffsrechts umgehen.
Link-Rechte	
Links anzeigen	Anzeigen der Links für diesen Ordner.
Links erstellen	Verknüpfen Sie den Ordner mit anderen Ordnern und Elementen.
Links ändern	Ändern von Links für diesen Ordner.
Links löschen	Löschen Sie einen Link mit diesem Ordner.

Verwandte Referenz

Zugriffsrechte und Berechtigungen

Zugriffsrechte für untergeordnete Ordner

Bei Auswahl des Knotens **Untergeordnete Ordner** im Dialogfeld **Ordner - Zugriffsrechte** werden die verfügbaren Rechte für die Unterordner des ausgewählten Ordners übernommen. Der Knoten **Untergeordnete Ordner** kann auch in den Dialogfeldern **Ansicht - Zugriffsrechte** und **Projekt - Zugriffsrechte** gewählt werden. In diesen Fällen gelten die Rechte jedoch für alle Unterordner der aktuellen Ansicht bzw. alle Unterordner des Projekts.

In der folgenden Tabelle werden die Zugriffsrechte beschrieben, die verfügbar sind, wenn Sie den Knoten **Untergeordnete Ordner** in den Dialogfeldern **Projekt - Zugriffsrechte**, **Ansicht - Zugriffsrechte** oder **Ordner - Zugriffsrechte** wählen.

Dieses Zugriffsrecht...	Ermöglicht einem Benutzer oder einer Gruppe Folgendes auszuführen...
Allgemeine Rechte für Element	
Element und seine Eigenschaften anzeigen	Die Unterordner des gewählten Ordners bzw. der gewählten Projekt- oder Ansichtsordner können in der Ordnerhierarchie im linken Teilfenster angezeigt werden. Sie können außerdem die Register "Name" und "Ausschließen" im Dialogfeld "Eigenschaften" anzeigen, das Sie durch Auswahl von "Ordner > Eigenschaften" öffnen können. Die Anzeige des Registers "Historie" wird durch das Ordnerzugriffsrecht "Historie anzeigen" gesteuert.
Eigenschaften ändern	Ändern der Ordnereigenschaften in den Registern "Name" und "Ausschließen" für Unterordner. Zu den Eigenschaften gehören der Ordnername, die Beschreibung, die Verwendung von geerbten und lokalen Ausschlusslisten sowie der Inhalt der lokalen Ausschlussliste. Wenn der Unterordner kein Stammordner ist, gehören der Arbeitsordner und die Einstellungen für den alternativen Arbeitsordner zu den Ordnereigenschaften. Bei Stammordnern gehören die Arbeitsordner zu den Ansichtseigenschaften und werden durch dieses Zugriffsrecht nicht gesteuert.
Aus Ordner löschen	Löschen der Unterordner des ausgewählten Ordners bzw. der ausgewählten Projekt- oder Ansichtsordner aus ihren übergeordneten Ordnern. Beachten Sie, dass Sie einen Ordner auch löschen können, wenn Sie über das Recht verfügen, einen der übergeordneten Ordner dieses Ordners zu löschen.
Elementzugriffsrechte ändern	Ändern Sie die Zugriffsrechte für die Unterordner des gewählten Ordners bzw. für die Ordner des gewählten Projekts oder der gewählten Ansicht. Stellen Sie sicher, dass Sie auch weiterhin zu den Benutzern gehören, die Zugriffsrechte ändern können, wenn Sie diese Einstellung ändern.
Historie anzeigen	Anzeigen des Registers **Historie** durch Auswählen von **Ordner ▸ Eigenschaften**. Dieses Recht gilt für die Unterordner des gewählten Ordners bzw. der Ordner des ausgewählten Projekts oder der ausgewählten Ansicht.
Wartung durchführen	Ändern der Revisionskommentare für zurückliegende Revisionen.
Exklusive Sperren einstellen	Sperren Sie untergeordnete Ordnerexklusiv.
Exklusive Sperren außer Kraft setzen	Entfernen Sie die exklusive Sperre eines anderen Benutzers für die untergeordneten Ordner.

Label-Rechte	
Ansichts-Labels anhängen/anpassen	Fügen Sie ein Ansichts-Label zu den Unterordnern des ausgewählten Ordners bzw. zu den Ordnern des des ausgewählten Projekts oder der ausgewählten Ansicht hinzu. Verschieben Sie ein Ansichts-Label von einer Revision eines Unterordners zu einer anderen. Durch dieses Recht wird die direkte Änderung von Ansichts-Labels von Unterordnern auf Ordnerebene gesteuert. Benutzer können neu erstellte Ansichts-Labels weiterhin an Unterordner anhängen.
Ansichts-Labels lösen	Entfernen Sie ein Ansichts-Label von den Unterordnern des ausgewählten Ordners bzw. von den Ordnern des ausgewählten Projekts oder der ausgewählten Ansicht. Beachten Sie, dass Benutzer, die Ansichts-Labels löschen können, auch Ansichts-Labels von den Unterordnern lösen können, indem sie das Label aus der Ansicht löschen und somit die Einstellung dieses Zugriffsrechts umgehen.
Revisions-Labels anhängen/anpassen	Fügen Sie ein Revisions-Label zu den Unterordnern des ausgewählten Ordners bzw. zu den Ordnern des ausgewählten Projekts oder der ausgewählten Ansicht hinzu. Verschieben Sie ein Revisions-Label von einer Revision eines Unterordners zu einer anderen. Durch dieses Recht wird die direkte Änderung von Revisions-Labels von Unterordnern auf Ordnerebene gesteuert.
Revisions-Labels lösen	Entfernen Sie ein Revisions-Label von den Unterordnern des ausgewählten Ordners bzw. von den Ordnern des ausgewählten Projekts oder der ausgewählten Ansicht. Beachten Sie, dass Benutzer, die Revisions-Labels löschen können, auch Revisions-Labels von den Ordnern lösen können, indem sie das Label aus der Ansicht löschen und somit die Einstellung dieses Zugriffsrechts umgehen.
Link-Rechte	
Links anzeigen	Anzeigen der Links mit den Unterordnern des ausgewählten Ordners bzw. der Ordner des ausgewählten Projekts oder der ausgewählten Ansicht.
Links erstellen	Verknüpfen Sie die Unterordner des gewählten Ordners bzw. die Ordner des gewählten Projekts oder der gewählten Ansicht mit anderen Ordnern oder Elementen.
Links ändern	Ändern eines Links mit den Unterordnern des gewählten Ordners bzw. des gewählten Projekt- oder Ansichtsordners.
Links löschen	Löschen Sie eine Verknüpfung einem Unterordner des ausgewählten Ordners bzw. mit einem Ordner des ausgewählten Projekts oder der ausgewählten Ansicht.
Allgemeine Rechte für Element-Container	
Ordner erstellen	Erstellen von Ordnern in übergeordneten Ordnern, Ansichten oder Projekten, für die diese Option im Dialogfeld **Zugriffsrechte > Untergeordnete Ordner** aktiviert ist.
Element vom übergeordneten Ordner gemeinsam nutzen/daraus verschieben	Gemeinsames Nutzen oder Verschieben von Ordnern in übergeordneten Ordnern, Ansichten oder Projekten, für die diese Option im Dialogfeld "Zugriffsrechte >

	Untergeordnete Ordner" aktiviert ist. Beachten Sie, dass die für den Ordner und seinen Inhalt festgelegten Zugriffsrechte sowie alle festgelegten Rechte für bestimmte Unterordner -und Elemente innerhalb dieses Zweigs der Ordnerhierarchie für den neuen Ordner erhalten bleiben.
Ordnerverhalten oder -konfiguration ändern	Ändern des Verzweigungsverhaltens und der Konfiguration von Ordnern in übergeordneten Ordnern, Ansichten oder Projekten, für die die entsprechende Option im Dialogfeld **Zugriffsrechte** im Knoten "Untergeordnete Ordner" aktiviert ist.

Verwandte Referenz

Zugriffsrechte und Berechtigungen

Datei - Zugriffsrechte

Wenn Sie das Dialogfeld **Datei - Zugriffsrechte** öffnen und den Knoten **Datei** wählen, gelten die Rechte nur für die ausgewählte Datei.

Die Zugriffsrechte für Dateien sind auch in den Dialogfeldern **Ordner - Zugriffsrechte**, **Ansicht - Zugriffsrechte** und **Projekt - Zugriffsrechte** verfügbar. In diesen Fällen gelten die Rechte jedoch nicht für eine einzelne Datei, sondern für alle Dateien der ausgewählten Ordner, Ansichten oder Projekte. Nur in diesen Dialogfeldern sind die folgenden Zugriffsrechte auf Containerebene verfügbar:

- Dateien hinzufügen
- Element vom übergeordneten Ordner gemeinsam nutzen/daraus verschieben
- Elementverhalten oder -konfiguration ändern

In den folgenden Abschnitten werden die Zugriffsrechte beschrieben, die über die Knoten **Datei** in den Dialogfeldern **Projekt - Zugriffsrechte**, **Ansicht - Zugriffsrechte**, **Ordner - Zugriffsrechte** und **Datei - Zugriffsrechte** verfügbar sind.

Allgemeine Rechte für Element

Im folgenden Abschnitt werden die allgemeinen Rechte für ein Element beschrieben.

Dieses Zugriffsrecht...	Ermöglicht einem Benutzer oder einer Gruppe Folgendes auszuführen...
Element und seine Eigenschaften anzeigen	Anzeigen von Dateien in der Dateiliste (oberes Teilfenster). Wählen Sie **Datei ▸ Eigenschaften**, um die Eigenschaften anzuzeigen.
Eigenschaften ändern	Ändern der Dateieigenschaften. Folgende Eigenschaften können bearbeitet werden: Archiv- oder Dateiname, Beschreibung, Bit-Einstellung für ausführbare Dateien (nur sinnvoll für Nicht-Windows-Plattformen), Komprimierung, Speicheroptionen und benutzerdefinierte Eigenschaften. Durch Verwendung eines alternativen Eigenschaftseditors (APE) können die veränderbaren Eigenschaften und vor allem die Benutzer, die Änderungen vornehmen dürfen, weiter eingeschränkt werden.
Aus Ordner löschen	Löschen von Dateien aus ihren Ordnern.
Elementzugriffsrechte ändern	Ändern der Zugriffsrechte für die Dateien. Stellen Sie sicher, dass Sie auch weiterhin zu den Benutzern gehören, die Zugriffsrechte ändern können, wenn Sie diese Einstellung ändern.
Historie anzeigen	Anzeigen der Dateihistorie im Teilfenster "Historie".
Wartung durchführen	Ändern der Revisionskommentare für zurückliegende Revisionen.
Exklusive Sperren einstellen	Exklusives Sperren von Dateien.
Exklusive Sperren außer Kraft setzen	Entfernen der exklusiven Dateisperre eines anderen Benutzers.

Label-Rechte

Im folgenden Abschnitt werden Label-Rechte beschrieben.

Dieses Zugriffsrecht...	Ermöglicht einem Benutzer oder einer Gruppe Folgendes auszuführen...
Ansichts-Labels anhängen/anpassen	Hinzufügen von Ansichts-Labels für diese Dateien. Verschieben von Ansichts-Labels von einer Revision zu einer anderen. Durch dieses Recht wird die direkte Änderung von Ansichts-Labels für die Dateien auf der Elementebene gesteuert. Benutzer können den Dateien dennoch weiterhin neu erstellte Ansichts-Labels zuweisen.

Ansichts-Labels lösen	Entfernen von Ansichts-Labels dieser Dateien. Beachten Sie, dass Benutzer, die Ansichts-Labels löschen können, auch Ansichts-Labels von den Dateien lösen können, indem sie das Label aus der Ansicht löschen und somit die Einstellung dieses Zugriffsrechts umgehen.
Revisions-Labels anhängen/anpassen	Hinzufügen von Revisions-Labels für diese Dateien. Verschieben von Revisions-Labels von einer Revision zu einer anderen. Durch dieses Recht wird die direkte Änderung von Revisions-Labels für die Dateien auf der Elementebene gesteuert. So kann verhindert werden, dass Benutzer Dateien mit zugewiesenen Revisions-Labels einchecken können.
Revisions-Labels lösen	Entfernen von Revisions-Labels dieser Dateien. Beachten Sie, dass Benutzer, die Revisions-Labels löschen können, auch Revisions-Labels von den Dateien lösen können, indem sie das Label aus der Ansicht löschen und somit die Einstellung dieses Zugriffsrechts umgehen.

Link-Rechte

Im folgenden Abschnitt werden Link-Rechte beschrieben.

Dieses Zugriffsrecht...	Ermöglicht einem Benutzer oder einer Gruppe Folgendes auszuführen...
Links anzeigen	Anzeigen der Links für diese Dateien.
Links erstellen	Verknüpfen der Dateien mit anderen Elementen.
Links ändern	Ändern von Links für diese Dateien.
Link löschen	Löschen von Links mit diesen Dateien.

Dateispezifische Rechte

Im folgenden Abschnitt werden die dateispezifischen Rechte beschrieben.

Dieses Zugriffsrecht...	Ermöglicht einem Benutzer oder einer Gruppe Folgendes auszuführen...
Datei einchecken	Einchecken der Dateien.
Datei auschecken	Auschecken der Dateien.

Allgemeine Rechte für Element-Container

Im folgenden Abschnitt werden die allgemeinen Rechte für Element-Container beschrieben.

Dieses Zugriffsrecht...	Ermöglicht einem Benutzer oder einer Gruppe Folgendes auszuführen...
Dateien hinzufügen	Hinzufügen von Dateien zu Ordnern, Ansichten oder Projekten, für die die entsprechende Option im Dialogfeld **Datei - Zugriffsrechte** aktiviert ist. Dieses Recht wird nur im Dialogfeld **Datei - Zugriffsrechte** eines Ordners, einer Ansicht oder eines Projekts angezeigt.
Element vom übergeordneten Ordner gemeinsam nutzen/daraus verschieben	Gemeinsames Nutzen oder Verschieben von Dateien in Ordnern, Ansichten oder Projekten, für die diese Option im Dialogfeld **Datei - Zugriffsrechte** aktiviert ist. Dieses Recht wird nur im Dialogfeld **Datei - Zugriffsrechte** eines Ordners, einer Ansicht oder eines Projekts angezeigt. Beachten Sie, dass die festgelegten Zugriffsrechte für eine Datei im neuen

	Ordner erhalten bleiben, wenn diese verschoben oder gemeinsam genutzt wird.
Ordnerverhalten oder -konfiguration ändern	Ändern des Verzweigungsverhaltens und der Konfiguration von Dateien in Ordnern, Ansichten oder Projekten, für die diese Option im Dialogfeld **Zugriffsrechte - Datei** aktiviert ist. Dieses Recht wird nur im Dialogfeld **Datei - Zugriffsrechte** eines Ordners, einer Ansicht oder eines Projekts angezeigt.

Verwandte Referenz

Zugriffsrechte und Berechtigungen

Allgemeine Elementzugriffsrechte ändern

In den folgenden Tabelle werden die Zugriffsrechte beschrieben, die über den Knoten **Datei** in den Dialogfeldern **Projekt - Zugriffsrechte**, **Ansicht - Zugriffsrechte**, **Ordner - Zugriffsrechte** und **Datei - Zugriffsrechte** verfügbar sind.

Dieses Zugriffsrecht...	Ermöglicht einem Benutzer oder einer Gruppe Folgendes auszuführen...
Element und seine Eigenschaften anzeigen	Anzeigen von Dateien in der Dateiliste (oberes Teilfenster). Wählen Sie **Datei ▸ Eigenschaften**, um die Eigenschaften anzuzeigen.
Eigenschaften ändern	Ändern der Dateieigenschaften. Folgende Eigenschaften können bearbeitet werden: Archiv- oder Dateiname, Beschreibung, Bit-Einstellung für ausführbare Dateien (nur sinnvoll für Nicht-Windows-Plattformen), Komprimierung, Speicheroptionen und benutzerdefinierte Eigenschaften. Durch Verwendung eines alternativen Eigenschaftseditors (APE) können die veränderbaren Eigenschaften und vor allem die Benutzer, die Änderungen vornehmen dürfen, weiter eingeschränkt werden.
Aus Ordner löschen	Löschen von Dateien aus ihren Ordnern.
Elementzugriffsrechte ändern	Ändern der Zugriffsrechte für die Dateien. Stellen Sie sicher, dass Sie auch weiterhin zu den Benutzern gehören, die Zugriffsrechte ändern können, wenn Sie diese Einstellung ändern.
Historie anzeigen	Anzeigen der Dateihistorie im Teilfenster "Historie".
Wartung durchführen	Ändern der Revisionskommentare für zurückliegende Revisionen.
Exklusive Sperren einstellen	Exklusives Sperren von Dateien.
Exklusive Sperren außer Kraft setzen	Entfernen der exklusiven Dateisperre eines anderen Benutzers.

Verwandte Referenz

Zugriffsrechte und Berechtigungen

Zugriffsrechte für Heraufstufungsstatuswerte

Jede Ansicht verfügt über einen eigenen Satz von Heraufstufungsstatuswerten. Der Zugriff auf diese Statuswerte wird vom Recht "Heraufstufungsmodell festlegen" gesteuert, das im Ansichtsknoten des Dialogfelds "Zugriffsrechte" auf Ansichts- und Projektebene festgelegt werden kann. Benutzer mit dem Recht zum Festlegen eines Heraufstufungsmodells können beispielsweise folgende Aktionen für das Heraufstufungsmodell ausführen: Statuswerte erstellen und löschen, Eigenschaften von Statuswerten bearbeiten und ein Label auf einen anderen Status heraufstufen. Die Heraufstufung ist der Bearbeitung von Eigenschaften untergeordnet. Benutzer mit dem Recht zum Bearbeiten der Eigenschaften können einen Status auch heraufstufen und die Statuswerte in einer Ansicht neu anordnen.

Zugriffsrechte, die den Zugriff auf einzelne Heraufstufungsstatuswerte steuern. Diese allgemeinen Rechte für Objekte und spezifischen Rechte für Heraufstufungsstatuswerte können im Knoten "Heraufstufungsstatus" des Dialogfelds "Zugriffsrechte" auf Ansichts- und Projektebene festgelegt werden. Sie werden außerdem bei den Zugriffsrechten für einzelne Heraufstufungsstatuswerte angezeigt. Die Rechte für einen einzelnen Heraufstufungsstatus werden auf der Statusebene und, falls nötig, weiter auf der Ansichtsebene und eventuell auf der Projektebene geprüft. Wenn einem Benutzer ein bestimmtes Zugriffsrecht auf einer Ebene gewährt wird, muss die folgende Ebene nicht geprüft werden.

Wird ein Zugriffsrecht auf Ansichtsebene gewährt, gilt es für alle Statuswerte der Ansicht, sofern der Zugriff auf Statusebene nicht verweigert wird. Wird ein Zugriffsrecht auf Projektebene gewährt, gilt es für alle Statuswerte in allen Ansichten des Projekts, sofern der Zugriff auf Status- oder Ansichtsebene nicht verweigert wird.

Dieses Zugriffsrecht...	Ermöglicht einem Benutzer oder einer Gruppe Folgendes auszuführen...
Objektzugriffsrechte ändern	Ändern Sie die Zugriffsrechte für einen einzelnen Heraufstufungsstatus. Stellen Sie sicher, dass Sie auch weiterhin zu den Benutzern gehören, die Zugriffsrechte ändern können, wenn Sie diese Einstellung ändern. Dieses Recht ist ein allgemeines Zugriffsrecht für Objekte. Nachdem Sie einen neuen Heraufstufungsstatus erstellt haben, müssen Sie das Dialogfeld "Heraufstufung" verlassen und erneut öffnen, um Zugriffsrechte für den neuen Status festlegen zu können.
Label-Zuweisung ändern	Ändern Sie Labels, die einem einzelnen Status zugewiesen sind, durch Klicken auf den Schalter Heraufstufen oder durch Bearbeiten der Label-Eigenschaften. Benutzer können keine weiteren Eigenschaften für den Status bearbeiten, wenn sie nicht über das Zugriffsrecht "Heraufstufungsmodell festlegen" verfügen, das im Knoten "Ansicht" verfügbar ist. Dieses Recht ist ein spezifisches Zugriffsrecht für Heraufstufungsstatuswerte.

Verwandte Referenz

Zugriffsrechte und Berechtigungen

Komponentenzugriffsrechte

Wenn Sie auf Serverebene über das Zugriffsrecht "Zugriffsrechte für Komponenten verwalten" verfügen, können Sie auf Komponentenebene Zugriffsrechte für alle geöffneten Komponenten festlegen.

Im Folgenden finden Sie eine Beschreibung der Komponentenzugriffsrechte.

Dieses Zugriffsrecht...	Ermöglicht einem Benutzer oder einer Gruppe Folgendes auszuführen...
Öffentliche Filter erstellen	Erstellen von öffentlichen Filtern für die Komponente.
Öffentliche Abfragen erstellen	Erstellen von öffentlichen Abfragen für die Komponente.

Verwandte Referenz

Zugriffsrechte und Berechtigungen

Filterzugriffsrechte auf Komponentenebene

Im Folgenden werden die Filterzugriffsrechte auf Komponentenebene beschrieben:

Dieses Zugriffsrecht	Ermöglicht einem Benutzer oder einer Gruppe Folgendes auszuführen...
Objekt und seine Eigenschaften anzeigen	Anzeigen von öffentlichen Filtern für diese Komponente in der Filterliste (Symbolleiste) und ihrer Eigenschaften im Dialogfeld "Filter".
Eigenschaften ändern	Ändern der Eigenschaften von öffentlichen Filtern für die Komponente. Die Eigenschaften, die für einen Filter geändert werden können, sind die Liste angezeigter Felder, die Regeln für das Sortieren und Gruppieren, die mit der Komponente verknüpfte Abfrage und der Kontext (die Elemente der Komponente, auf die sie angewendet werden).
Objekt löschen	Löschen von öffentlichen Filtern für die Komponente aus der Filterliste.
Objektzugriffsrechte ändern	Ändern der Zugriffsrechte für öffentliche Filter der Komponente.

Verwandte Referenz

Zugriffsrechte und Berechtigungen

Zugriffsrechte für einzelne Filter

Die einzelnen Filterzugriffsrechte werden in der folgenden Tabelle beschrieben:

Dieses Zugriffsrecht...	Ermöglicht einem Benutzer oder einer Gruppe Folgendes auszuführen...
Objekt und seine Eigenschaften anzeigen	Der Filter wird in der Filterliste (in der Symbolleiste) und die Eigenschaften werden im Dialogfeld **Filter** angezeigt.
Eigenschaften ändern	Ändern Sie die Filtereigenschaften. Folgende Eigenschaften können für den Filter geändert werden: die Liste angezeigter Felder, die Regeln für das Sortieren und Gruppieren, die mit dem Filter verknüpfte Abfrage und der Kontext (die Elemente der Komponente, auf die er angewendet werden kann).
Objekt löschen	Löschen des Filters aus der Filterliste.
Objektzugriffsrechte ändern	Ändern Sie die Zugriffsrechte für den Filter.

Verwandte Referenz

Zugriffsrechte und Berechtigungen

Abfragezugriffsrechte auf Komponentenebene

In der folgenden Tabelle werden die Abfragezugriffsrechte auf Komponentenebene beschrieben:

Dieses Zugriffsrecht...	Ermöglicht einem Benutzer oder einer Gruppe Folgendes auszuführen...
Objekt und seine Eigenschaften anzeigen	Öffentliche Abfragen werden im Dialogfeld "Abfragen" und ihre Eigenschaften im Dialogfeld "Abfrage bearbeiten" angezeigt.
Eigenschaften ändern	Ändern der Eigenschaften von öffentlichen Abfragen für die Komponente. Folgende Eigenschaften können verändert werden: der Name und die Bedingungen der Abfrage.
Objekt löschen	Löschen von öffentlichen Abfragen für die Komponente aus der Abfrageliste.
Objektzugriffsrechte ändern	Ändern der Zugriffsrechte für öffentliche Abfragen der Komponente.

Verwandte Referenz

Zugriffsrechte und Berechtigungen

Zugriffsrechte für einzelne Abfrage

In der folgenden Tabelle werden die einzelnen Abfragezugriffsrechte beschrieben:

Dieses Zugriffsrecht...	Ermöglicht einem Benutzer oder einer Gruppe Folgendes auszuführen...
Objekt und seine Eigenschaften anzeigen	Die Abfrage wird im Dialogfeld **Abfragen** angezeigt. Zeigen Sie die Eigenschaften der Abfrage im Dialogfeld **Abfrage bearbeiten** an.
Eigenschaften ändern	Ändern Sie die Eigenschaften der Abfrage. Die Eigenschaften, die verändert werden können, sind der Name und die Bedingungen der Abfrage.
Objekt löschen	Löschen der Abfrage aus der Abfrageliste.
Objektzugriffsrechte ändern	Ändern der Zugriffsrechte für diese Abfrage.

Verwandte Referenz

Zugriffsrechte und Berechtigungen

Index